普通高等学校本科专业设置申请表

校长签字：

学校名称（盖章）：广东东软学院



学校主管部门：广东省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-17

专业负责人：罗先录

联系电话：17722776161

教育部制

1.学校基本情况

学校名称	广东东软学院	学校代码	12574
主管部门	广东省	学校网址	http://www.nuit.edu.cn/
学校所在省市区	广东佛山南海软件科技园	邮政编码	528200
学校办学基本类型	☐教育部直属院校 ☐其他部委所属院校 ☑地方院校 ☐公办 ☑民办 ☐中外合作办学机构		
已有专业学科门类	☐哲学 ☐经济学 ☐法学 ☐教育学 ☑文学 ☐历史学 ☐理学 ☑工学 ☐农学 ☐医学 ☑管理学 ☑艺术学		
学校性质	☐综合 ☑理工 ☐农业 ☐林业 ☐医药 ☐师范 ☐语言 ☐财经 ☐政法 ☐体育 ☐艺术 ☐民族		
曾用名	南海东软信息技术职业学院		
建校时间	2002	首次举办本科教育年份	2014年
通过教育部本科教学评估类型	尚未通过本科教学评估	通过时间	-
专任教师总数	625	专任教师中副教授及以上职称教师数	146
现有本科专业数	23	上一年度全校本科招生人数	2409
上一年度全校本科毕业人数	2165		
学校简要历史沿革	广东东软学院是经教育部批准设立的全日制普通高等本科学校，创办于2002年，前身是南海东软信息技术职业学院。2014年学校升格为普通本科学校，更名为广东东软学院，共设置了23个本科专业，涵盖工学、管理学、艺术学、文学4个学科门类。2018年通过新建本科院校学士学位授予单位评估。		
学校近五年专业增设、停招、撤并情况	近五年增设专业如下： 2020年增设软件工程（中外合作办学）专业； 2021年增设健康服务与管理专业、人工智能专业、计算机科学与技术专业； 2022年增设机器人工程专业。 近五年停招、撤并专业：无		

2. 申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	计算机学院		
学校现有相近专业情况			
相近专业1专业名称	网络工程	开设年份	2014年
相近专业2专业名称	-	开设年份	-
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	网络空间安全专业毕业生的就业领域广泛，主要覆盖国家关键信息基础设施保护、数字经济核心产业支撑与公共安全治理等关键方向。一方面，大量毕业生进入专业网络安全企业，承担渗透测试、漏洞挖掘、威胁情报分析、安全产品研发等技术岗位，为政府、企业客户提供专业安全服务。另一方面，互联网公司与IT企业亦为重要去向，毕业生在此从事云计算、大数据平台、移动应用等系统的安全设计、运行维护与风险防控。随着数字化转型的深入，金融、能源、电信、智能制造等行业对安全运维、合规审计、工控系统防护及应急响应能力提出更高要求，吸纳大量具备复合能力的网络安全人才。在公共安全领域，毕业生也可进入党政机关、公安、国家安全等单位，参与等级保护、电子取证、网络反恐等关键任务，维护国家安全与社会稳定。
人才需求情况	2016年《国家网络空间安全战略》提出“到2035年建成世界网络强国”，2017年《网络安全法》要求关键信息基础设施运营者配备专职安全人员，2022年《“十四五”国家信息化规划》明确“2025年初步建成网络安全人才培养体系”。教育部《2024年网络安全产业人才发展报告》显示，2027年网络安全人才缺口将达327万，而高校年培养规模仅3万，供需比1:5，缺口规模居新工科首位。用人单位岗位已从传统渗透测试、安全运维扩展至云原生安全、AI安全、车联网安全、工业控制安全、隐私计算等新兴领域，形成

	“橄榄形”需求结构：奇安信未来三年年均新增200－300人，阿里安全部400人，腾讯500人，华为200人；国家电网三年300人，中国工商银行年均80人，中央网信办及公安系统年均200－300人，复合型人才成为刚需。 广东东软学院依托东软集团产业优势，2018 年与奇安信共建“网络空间安全产业学院”，建成攻防靶场和在线实验平台，形成“课程共建—师资共享—项目共研—证书共认”的协同育人闭环，可同时承载课程实验、红蓝对抗、CTF 集训及企业真实项目。同时与广东红帽网络科技有限公司签订校企实践与就业基地合作协议，成功打造广东省校外实践基地-红帽工程，并获得了鹏城靶场的授权成为鹏城靶场广东东软学院分靶场。学生在校期间有机会参加如全运会、广交会、粤盾等重大网络安保任务，在盘古石杯、美亚杯、FIC大赛等网络安全类竞赛中获得国家一等奖、二等奖等多个奖项，充分展现了学校在网络安全实践教学方面的突出成果和学生扎实的专业素养。	
申报专业人才需求调研情况	年度招生人数	60
	预计升学人数	6
	预计就业人数	54
	奇安信科技集团有限公司	6
	北京神州绿盟信息安全科技股份有限公司	6
	蓝盾信息安全技术股份有限公司	5
	东软集团股份有限公司	5
	广东科信安信息技术有限公司	4
	启明星辰信息技术集团股份有限公司	3
	广东广宇科技发展有限公司	2
	中科汇能科技有限公司	2
	深信服科技股份有限公司	1
	广东翌安科技有限公司	2
	广东安创信息科技开发有限公司	2

	佛山市伏宸信息科技有限公司	3
	广东安杰技术服务有限公司	2
	上海观安信息技术股份有限公司	2
	广州皓邦信息科技有限公司	3
	广东省信息安全测评中心	1
	永信至诚科技集团股份有限公司广东分公司	2
	广州睿丰数据服务有限公司	2
	北京中安国发信息技术研究院	1

4. 产业调研报告

网络空间安全行业产业调研报告

在"网络强国""数字中国"战略引领下，我国网络安全产业进入黄金发展期，2025 年市场规模将突破 800 亿元，年复合增长率达 20.5%，全球第一。与此同时，网络安全人才缺口超 70 万，高校年供给仅 3.2 万人，供需严重失衡。设立网络空间安全专业，既是服务国家安全战略的必然选择，也是支撑区域数字经济高质量发展的关键举措。为了响应这一需求，我院拟新开设网络空间安全专业。为此，我们对网络空间安全行业的市场现状、网络空间安全市场人才缺口情况、广东省内高校网络空间安全专业的设置情况以及网络空间安全专业的就业前景进行了深入调研，现将调研结果总结如下。

1、网络空间安全行业发展现状

1.1 市场规模持续增长

随着中国经济环境平稳转段、网络安全相关政策法规和标准规范相继落地、网络安全治理日臻完善、网络安全技术加快迭代升级等正向激励效能显现，我国网络安全市场需求持续扩大，市场规模持续增长。根据 IDC 预测，中国网络安全市场规模从 2022 年的 123.5 亿元快速增长至 2027 年的 233.2 亿元，期间年复合增长率为 13.5%，高于全球平均水平。未来中国网络安全市场将更加成熟，在整体技术市场组成中，安全防御硬件设备逐步云化，网络安全软件和服务市场持续增长，五年复合增长率分别为 16.7%和 16.3%。



1.2 政策法规与国家战略支撑

网络安全是当今世界面临的重要挑战之一，各国纷纷制定了相关政策和法规来加强网络安全防护。在中国，网络安全已被列为国家重要战略，政府出台了一系列政策来加强网络安全防护和管理。

中国网络空间安全行业政策法规主要包括《网络安全法》、《数据安全法》、《个人信息保护法》等，以及相关的国家标准和规范。这些法规和标准共同构建了中国网络空间安全治理的法律框架，旨在维护国家网络安全、数据安全和个人信息安全。

《中华人民共和国网络安全法》于 2017 年 6 月 1 日起施行，是网络安全领域的基础性法律，明确了网络安全等级保护制度，规范了网络运营者的安全义务，并对网络信息安全、个人信息保护等作出了规定。《中华人民共和国数据安全法》于 2021 年 9 月 1 日起施行，旨在规范数据处理活动，保护数据安全，维护国家安全和公共利益，明确了数据分类分级保护、重要数据保护等制度。《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日起施行，旨在保护个人信息权益，规范个人信息处理活动，明确了个人信息处理规则、个人信息出境规则、个人信息权益保护等。《关键信息基础设施安全保护条例》进一步细化了关键信息基础设施的保护要求，明确了运营者在安全保护方面的责任和义务。

其次，中国政府成立了国家互联网信息办公室，负责统一协调全国网络安全工作，加强网络安全监管和管理。该机构制定了一系列网络安全标准和规范，推动各行业加强网络安全建设，提高网络安全防护水平。

此外，中国政府还加强了网络安全技术研发和人才培养。政府出台了一系列扶持政策，支持企业和高校开展网络安全技术研究，推动网络安全技术创新和应用。同时，政府还鼓励培养网络安全专业人才，加强网络安全人才队伍建设，提高网络安全防护能力。

总的来说，中国政府高度重视网络安全问题，通过制定相关政策和法规，加强网络安全管理和监管，推动网络安全技术研发和人才培养，积极参与国际网络安全合作，全面提升国家网络安全防护能力。网络安全已成为国家安全的重要组成部分，中国政府将继续加大力度，不断完善网络安全政策和措施，确保网络安全和信息安全。

我国及部分省市网络安全行业相关政策

发布时间	发布部门	政策名称	主要内容
2024年1月	工业和信息化部、公安部、自然资源部、住房和城乡建设部、交通运输部	关于开展智能网联汽车"车路云一体化"应用试点工作的通知	具有省级或市级智能网联汽车安全监测能力、运输安全保障能力、汽车网络安全和数据安全管理能力、安全隐患和突发事件处置能力等安全管理条件。
2024年4月	商务部	数字商务三年行动计划（2024-2026年）	守住安全底线，保障商务领域数据安全和网络安全，坚决维护国家主权、安全、发展利益，严格落实"三管三必须"责任，防范数字商务领域安全生产风险。
2024年5月	国家发展改革委、国家数据局、财政部等部门	关于深化智慧城市发展推进城市全域数字化转型的指导意见	加强城市数字空间安全管理，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系，提升通信网络韧性。
2024年11月	工业和信息化部等十二部门	5G规模化应用"扬帆"行动升级方案	完善通信网络安全防护管理，加快新兴行业5G终端安全、网络设备安全、数据安全、密码安全等关键技术研究，推动研制具备虚拟化、智能化、自适应能力的安全产品。
2024年12月	工业和信息化部、财政部、中国人民银行、金融监管总局	中小企业数字化赋能专项行动方案（2025—2027年)	全面增强中小企业数据与网络安全防护能力。引导中小企业建立健全网络和数据安全管理制度，促进态势感知、工业防火墙、入侵检测系统等安全产品部署应用。支持中小企业开展网络和数据安全演练，提升中小企业网络风险防御和处置能力。鼓励中小企业通过购买网络安全保险等方式降低安全风险。
2025年2月	工业和信息化部、市场监管总局	关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知	加强认证服务和管理。推动构建智能网联汽车质量认证体系，围绕组合驾驶辅助系统的数据安全、网络安全、功能安全、预期功能安全等领域积极推行自愿性认证，服务智能网联汽车产业健康发展。
2025年3月	国务院办公厅	关于做好金融"五篇大文章"的指导意见	加强数据安全、网络安全、信息科技外包、算法模型、新技术运用等风险管理，推进金融业关键信息基础设施信息技术创新应用。

1.3 网络安全代表企业与市场格局

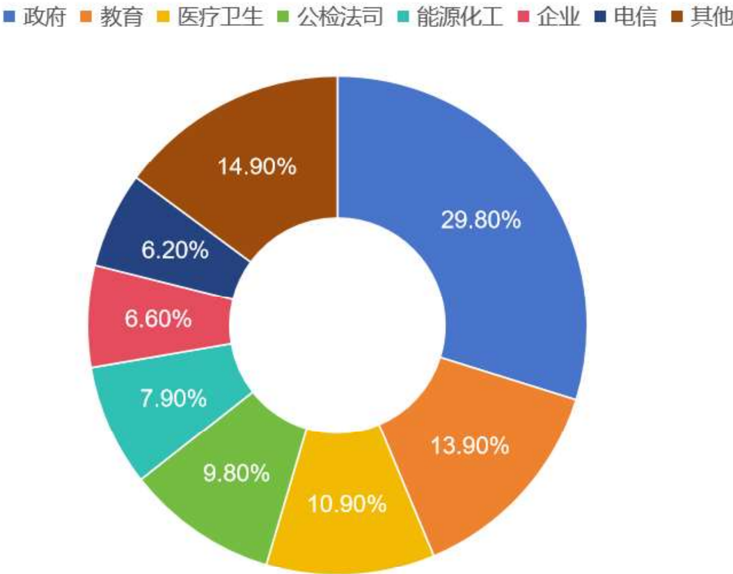
这些品牌在网络安全的生产和供应上占据了重要地位，不仅在国内市场有着广泛的影响力，也在国际市场上逐渐崭露头角。2025 年网络安全品牌排行榜的详细排名为奇安信、启明星辰、深信服 SANGFOR、天融信 TOPSEC、华为 HUAWEI、新华三 H3C、绿盟科技、安恒信息、腾讯安全、360 数字安全。

2025 年网络安全十大品牌排行榜

排名	品牌名称	企业名称	省份/地址
1	奇安信	奇安信科技集团股份有限公司	北京市
2	启明星辰	启明星辰信息技术集团股份有限公司	北京市
3	深信服SANGFOR	深信服科技股份有限公司	广东省
4	天融信TOPSEC	天融信科技集团股份有限公司	北京市
5	华为HUAWEI	华为投资控股有限公司	广东省
6	新华三H3C	新华三技术有限公司	浙江省
7	绿盟科技	绿盟科技集团股份有限公司	北京市
8	安恒信息	杭州安恒信息技术股份有限公司	浙江省
9	腾讯安全	深圳市腾讯计算机系统有限公司	广东省
10	360数字安全	三六零安全科技股份有限公司	北京市

1.4 网络安全项目分布领域

从项目数量分布来看，我国网络安全项目数量分布最多的政府，占比为 29.8%；其次为教育，占比为 13.9%；第三为医疗卫生，占比为 10.9%。



1.5 技术发展趋势与方向

网络安全行业是一个不断发展和变化的领域，随着网络技术的不断进步和网络攻击的不断增加，网络安全行业也在不断壮大和发展。以下是网络安全行业发展趋势的一些重要方面：

人工智能和机器学习在网络安全中的应用：随着人工智能和机器学习技术的不断发展，越来越多的网络安全公司开始将这些技术应用到网络安全领域中。人工智能和机器学习可以帮助网络安全专家更快速地识别和应对网络攻击，提高网络安全的效率和准确性。

云安全的重要性：随着云计算技术的普及和应用，云安全也变得越来越重要。网络安全公司需要不断研究和开发新的云安全解决方案，以应对云环境中的各种安全威胁。

物联网安全：随着物联网设备的普及和应用，物联网安全也成为一个备受关注的问题。网络安全公司需要研究和开发新的物联网安全解决方案，以保护物联网设备和数据的安全。

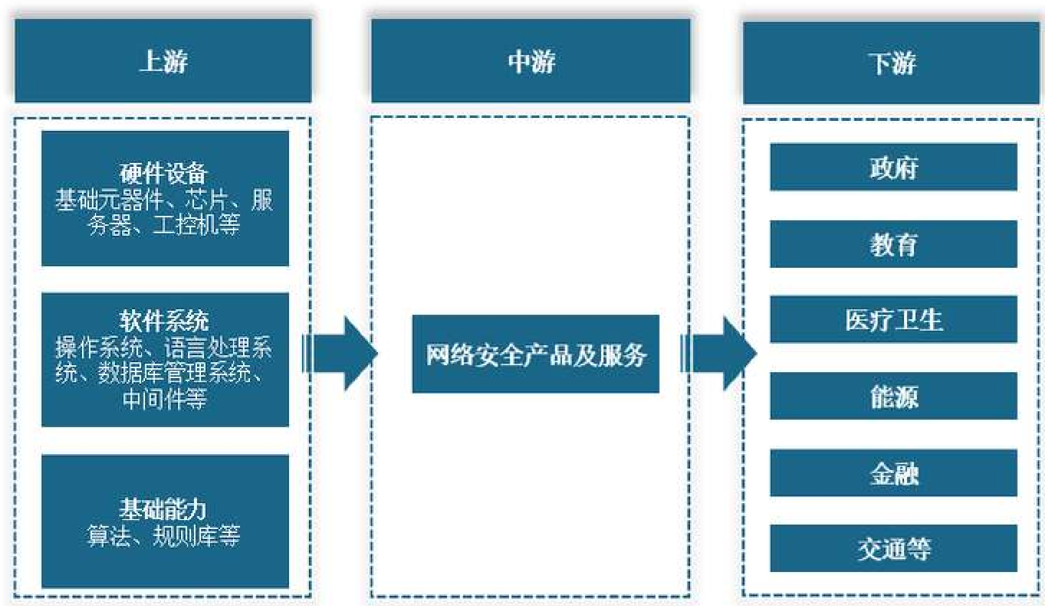
大数据安全：随着大数据技术的发展和应用，大数据安全也成为一个重要的问题。网络安全公司需要研究和开发新的大数据安全解决方案，以保护大数据的安全和隐私。

自动化安全工具的发展：随着网络安全威胁的不断增加，网络安全公司需要更快速、更高效地应对这些威胁。因此，自动化安全工具的发展变得越来越重要，可以帮助网络安全专家更快速地发现和应对网络攻击。

区块链技术在网络安全中的应用：区块链技术具有去中心化、不可篡改等特点，可以帮助提高网络安全的可信度和透明度。网络安全公司需要研究和开发新的区块链安全解决方案，以提高网络安全的水平。

1.6 网络安全产业链结构

从产业链来看，网络安全上游主要为硬件设备、软件系统和基础能力，其中硬件设备包括基础元器件、芯片、服务器、工控机等；软件系统包括操作系统、语言处理系统、数据库管理系统、中间件等；基础能力包括算法、规则库等。中游为网络安全产品及服务。下游为政府、教育、医疗卫生、能源、金融、交通等应用领域。



总的来说，网络空间安全行业是一个充满挑战和机遇的领域，网络空间安全公司需要不断跟上技术发展的步伐，研究和开发新的网络安全解决方案，以保护网络和数据的安全。随着网络技术的不断发展和网络攻击的不断增加，网络安全行业的发展前景将会更加广阔。

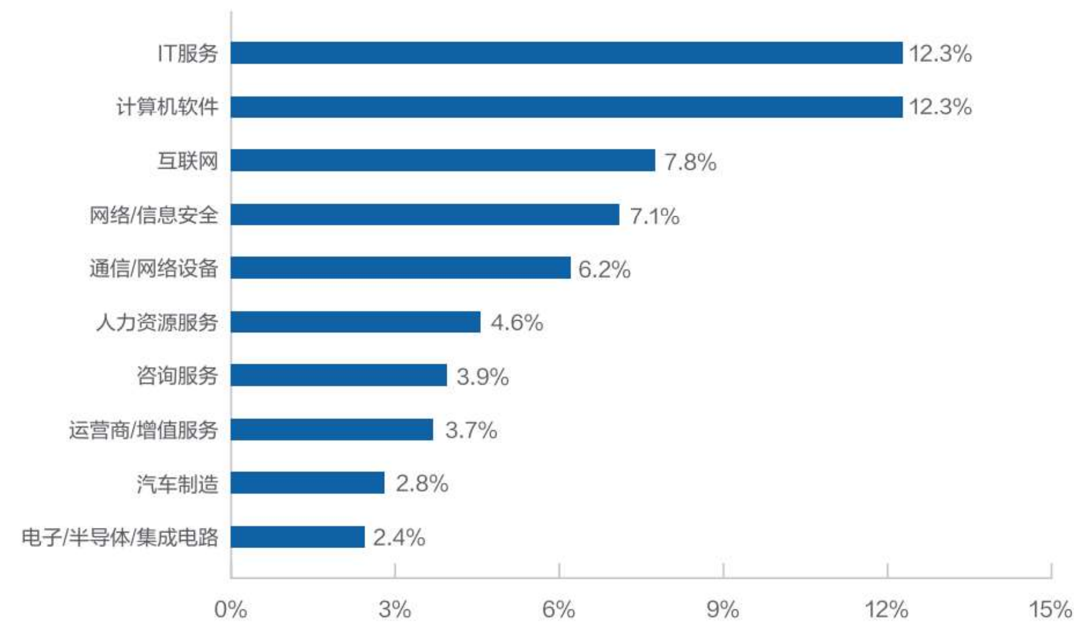
2、网络空间安全人才供需缺口分析

2.1 全国缺口持续扩大，供需矛盾尖锐化

基于工信部《网络安全产业人才发展报告（2023）》的权威数据显示，我国网络安全市场规模预计 2025 年将突破 800 亿元，年复合增长率保持在 15%以上。在数字经济与合规监管双轮驱动下，数据安全、云安全、AI 安全等新兴赛道迅速扩容，直接拉动了对安全研发、安全运维、数据治理、渗透测试等岗位的需求。然而，与高速增长的市场规模形成鲜明对比的是，2023 年网络安全相关专业本科毕业生仅约 3.2 万人，供需缺口超过 70 万，预计 2025 年行业人才缺口将达 140 万人，而高校年培养规模仅约 3 万人，供需比例严重失衡至不足 5%，院校供给端难以满足我国网络安全产业发展对人才的需要。且缺口呈逐年扩大趋势，报告明确将“整体供需失衡”列为产业人才发展的首要问题。而《网络安全人才实战能力白皮书》进一步预测，随着数字化转型的深入推进，2027 年该缺口可能扩大至 327 万人，人才供给的滞后性已成为制约网络安全产业高质量发展的关键瓶颈。

2.2 岗位职能与层级需求分化显著

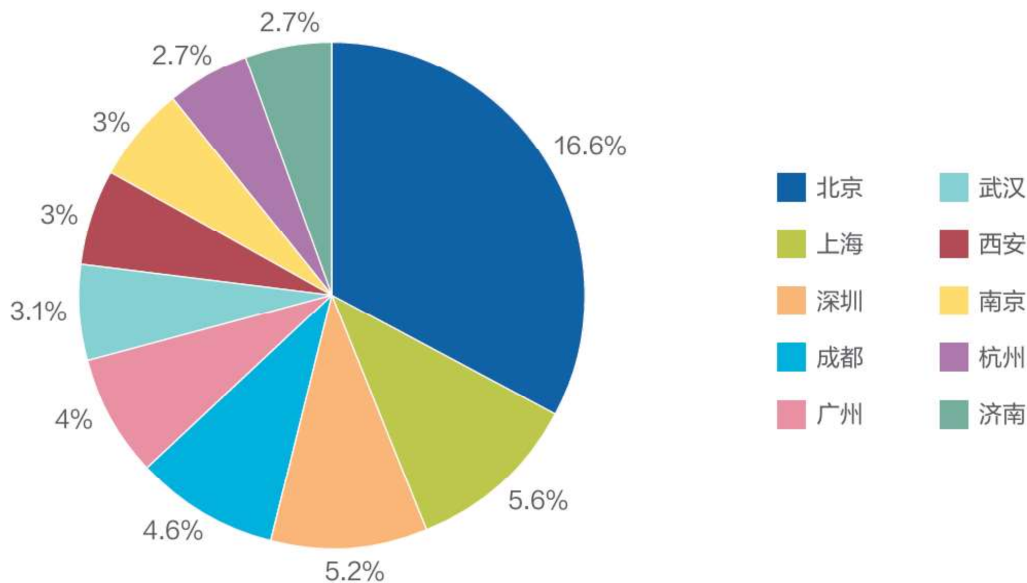
网络安全产业的发展推动了人才招聘需求的增长，也激活了相关领域的就业，带动了人才供给，不仅催生了大量新兴岗位，也对人才市场形成了“需求牵引—供给响应—再升级”的循环机制。根据智联招聘平台数据显示，2024 年招聘网络安全岗位数量最多的是 IT 服务行业和计算机软件行业，二者合计占比约为 24.6%。其次是互联网行业，占比约为 7.8%，网络/信息安全行业，占比约为 7.1%。此外，通信/网络设备、人力资源服务、咨询服务、运营商/增值服务、汽车制造等行业，也对网络安全人才有较大需求。下图为网络安全招聘职位行业分布。



网络安全招聘职位行业分布图

2.3 地域与行业需求高度集中

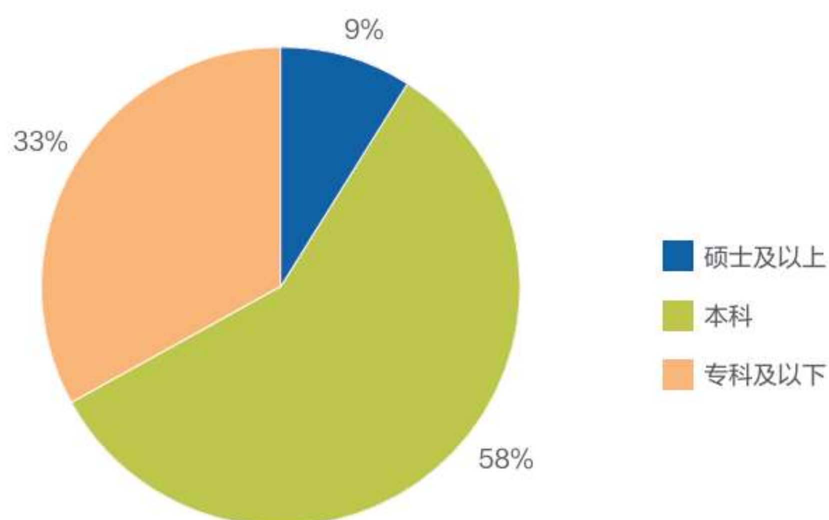
从城市来看，网络安全岗位需求比较多的城市主要集中在一线城市、新一线城市及省会城市等经济发达、科技创新活跃的地区。这些城市拥有较多的网络安全企业和机构，对网络安全人才的需求量较大。据智联招聘平台数据显示，在网络安全人才需求方面，北京的需求依旧最为旺盛，占比高达 16.6%。上海占比为 5.6%，深圳占比约为 5.2%，成都占比约为 4.6%，另外，广州、武汉、西安、南京等城市的招聘职位数占比也都超过了 3%。下图是网络安全招聘岗位数量占比 TOP10 城市。



网络安全招聘岗位数量占比 TOP10 城市

2.4 能力错配加剧企业用人成本

网络安全行业作为一个技术密集型领域，对从业人员的学历要求逐年升高。大多数招聘单位在招聘网络安全岗位时，要求应聘者具备本科及以上学历，并具备计算机科学与技术、信息安全、软件工程、网络与通信工程等相关专业背景。从学历要求来看，2024 年本科学历网络安全人才的招聘需求较高，招聘职位数占比为 58%。下图为网络安全岗位招聘学历要求分布。

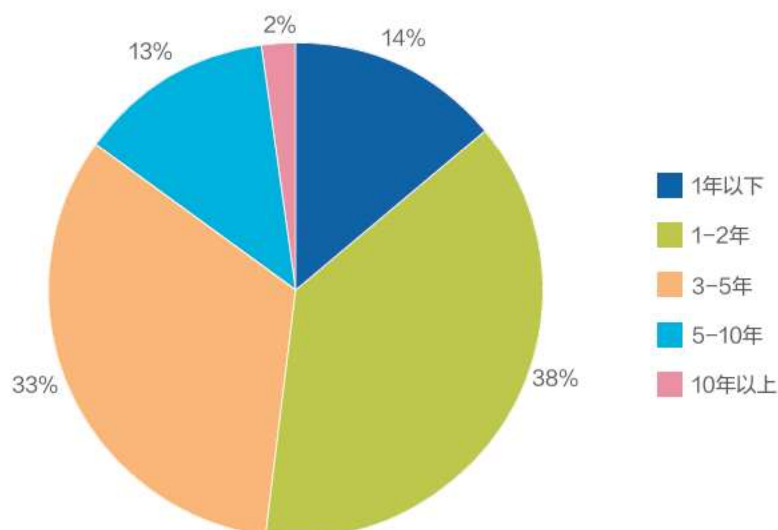


网络安全岗位招聘学历要求分布

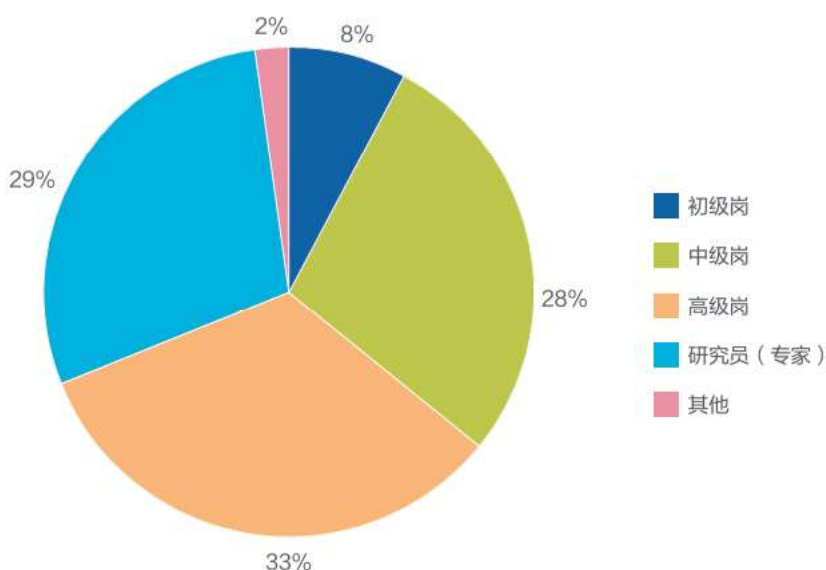
据智联招聘平台数据显示，工作类别方面，网络安全运营招聘职位数占比最高，达到29.4%。其次是网络安全建设、网络安全管理、数据安全、网络安全审计和评估，占比分别为 18.7%、17.6%、10.5%和 8.2%。下表为网络安全招聘岗位数量分布。

一级职能	二级职能	典型职位	占比
网络安全运营（29.4%）	网络安全运维	安全运维工程师	15.77%
	网络安全集成	集成方案解决师	7.80%
	网络安全应急响应	网络安全应急响应工程师	5.85%
网络安全建设（18.7%）	网络安全开发	网络安全开发师	11.79%
	网络安全架构	安全系统架构师	6.47%
	个人信息保护	/（无典型职位）	0.35%
	供应链安全	供应链安全管理	0.13%
网络安全管理（17.6%）	网络安全测试	安全测试工程师	8.38%
	网络安全合规	安全合规工程师	3.36%
	网络安全咨询	安全咨询工程师	2.85%
	网络安全规划	安全规划师	1.77%
	网络安全防护	安全等级保护测评师	1.29%
数据安全（10.5%）	数据安全体系	数据安全体系工程师	3.19%
	数据安全管理	数据管理师	3.34%
	数据安全评估	数据安全评估师	2.64%
	数据安全保护	数据安全保护工程师	1.01%
网络安全审计和评估（8.2%）	电子数据取证	电子数据取证师	0.28%
	网络安全分析	渗透测试/漏洞挖掘工程师	5.56%
	网络安全评估	网络安全评估师	2.36%
	网络安全认证	安全认证工程师	0.32%

网络安全岗位的工作经验往往与岗位的性质、工作技能紧密相关，招聘单位对网络安全人才的工作经验也越来越看重。很多企业在招聘时会优先考虑那些具有实际项目经验、能够迅速适应工作环境并解决问题的应聘者。工作经验方面，2024 年网络安全领域要求 1-2 年工作年限的招聘职位数占比为 38%，其次是要求 3-5 年的工作年限，占比达到 33%。下图为网络安全岗位的工作年限要求分布。

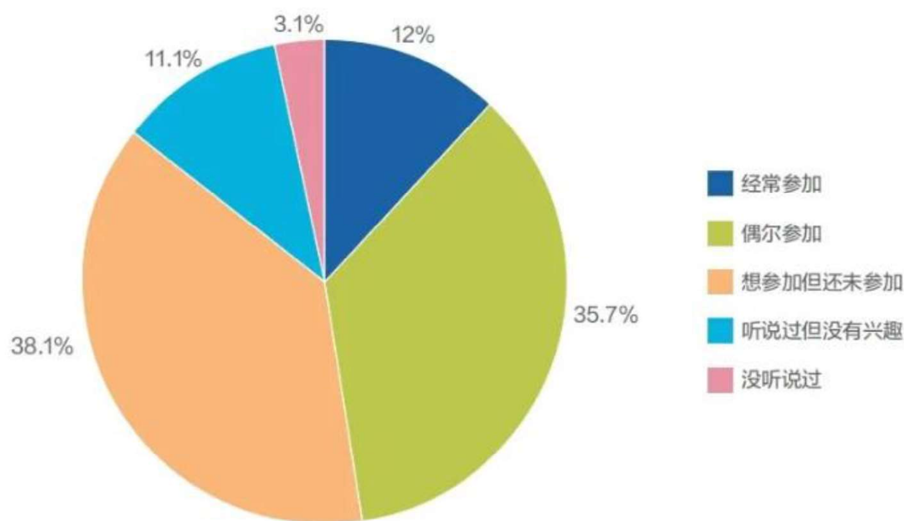


调研数据显示，受访者普遍认为所属公司随着业务发展，未来急需中、高级岗位的信息安全人员。从调研数据来看，受访者中认为急需高级、研究员（专家）岗位信息安全人员占比分别达到 33%和 29%。下图为未来网络信息安全岗位人才需求分布。



2.5 实战性需求不减，实战型人才更受青睐

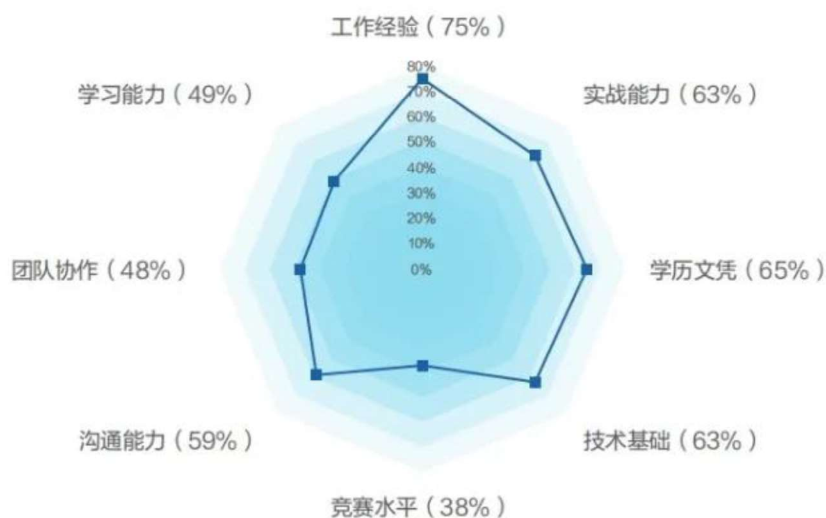
网络安全教育正向实用化、行业导向型转变。报告显示，设立网络安全专业的院校，近九成已建设网络安全实训室，为学生提供了良好的实践教学平台和实训环境。在网络安全专业课程教学过程中，企业讲师参与教学授课的院校占比 68.8%。可见，聘任具有行业实践经验的企业讲师参与教学，已成为大部分学校选择的教学方式



在校期间是否有参与过网络安全相关的竞赛

经调研数据显示，在校期间学生参加过网络安全相关竞赛的比重为 47.7%，其中包括经常参加竞赛的学生占比为 12.0%，偶尔参加的占比 35.7%。超过四成在校生参加过网安竞赛，提升实战能力占主导因素。

近年来，招聘单位也越来越重视应聘者的实战技能和工作经验。特别是在一些实践性强的岗位上，如渗透测试工程师、安全运维工程师等，应聘者的实际操作能力和项目经验往往比学历更加重要。一些招聘单位开始采用多元化的评价体系，除了学历和专业技能外，还会关注应聘者的沟通能力、团队协作能力、学习能力等非学历因素。



2024年用人单位对网络安全人才能力要求

综上可见，网络安全人才“百万缺口”已是制约行业发展的硬性约束。我校地处粤港澳大湾区核心，具备产业资源与学科基础，同时作为应用型大学，注重学生的实践能力的培养，增设网络空间安全本科专业恰逢其时，既可有效缓解区域人才供需失衡，又能为学生打开广阔就业通道。

3、广东省高校网络空间安全专业布局现状

《2023 网络安全人才市场状况研究报告》显示国内网络安全科技人才的市场需求累计增长达 40%，网络安全人才招聘需求城市排行中广州、深圳占到了全国需求总量的 18.7%。目前，广东已有 10 多所高校开网络安全相关本科专业。

	广东省分数线			招生人数		
学校名称	22 年	23 年	24 年	22 年	23 年	24 年
中山大学	638	651	未公布	33	44	61
暨南大学	614	625	未公布	27	27	未公布
惠州学院	522	523	未公布	未公布	未公布	未公布
广东技术师范大学	528	未公布	未公布	210	未公布	未公布
广州大学	581	585	未公布	70	89	未公布
东莞理工学院	557	未公布	未公布	53	未公布	未公布
广东外语外贸大学	561	574	未公布	未公布	未公布	未公布
广州软件学院	未公布	474	475	未公布	80	110
广州商学院	未公布	462	未公布	未公布	未公布	未公布
广东科技学院	未公布	未公布	未公布	未公布	未公布	未公布
成都东软学院				282	337	
大连东软学院						57/60

根据调研结果来看，广东省共有 162 所高校，其中 10 所高校开设了网络空间安全专业，占比 16.2%。从招生规模来看，广东省内高校网络空间安全专业的招生人数有逐年增加的趋势，反映出社会对网络安全人才的强烈需求。

网络空间安全人才培养，需要更多所高校参与其中，逐步完善网络安全人才培养体系，全面深化产学研融合，共同打造网络安全人才成长的“摇篮”。

4、网络空间安全专业就业前景

作为计算机类专业，网络空间安全专业毕业生除可胜任计算机类相关工作外，还可进入

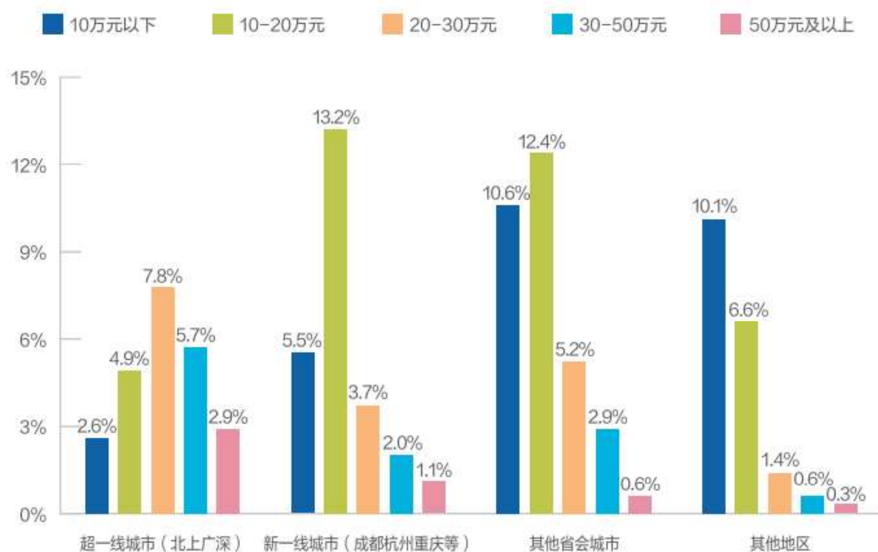
政府机关单位从事安全规划、安全管理和等级保护等相关工作，或在企业从事网络空间安全领域的技术开发与运维、安全管理、系统（产品）研发与运维、安全分析与设计、技术咨询与服务、项目管理等相关工作。



根据工信部发布的《网络安全产业人才发展报告》，网络安全产业人才需求还在高速增长，2021 年上半年，行业人才需求总量已经较去年同期增长了 39.87%，不少企业为了招到人才不惜付出高薪，2021 年网络安全领域的平均招聘薪酬已达到 22387 元/月，较去年同期提高了 4.85%。平均工资较全行业偏高的主要原因是大部分公司希望通过社会招聘网站招募经验足、技术强的人才。

根据麦可思就业蓝皮书数据显示：自 2014 届开始，信息安全专业成为薪资最高专业，并 连续 10 年位居毕业半年后月收入较高本科专业榜首，2023 届毕业生月收入为 7756 元。

因城市发展水平、影响力、网络安全企业规模等因素，超一线城市（北上广深）的薪资收入分布在 20-30 万及 30-50 万区间较多，10 万元以下比例最低，50 万元及以上在同其他城市相比时比例最高。新一线城市（成都杭州重庆等）的薪资收入主要集中在 10-20 万区间。其他省会城市的薪资收入集中在 10 万元以下及 10-20 万两个区间。其他地区的薪资收入比例大多在 10 万元以下。



综上而言，当前网络安全已成为国家安全体系的战略支柱，面对数字化转型浪潮下日益复杂的安全威胁，尤其是粤港澳大湾区等数字经济高地面临的专业人才结构性缺口，设立网络空间安全本科专业刻不容缓。该专业将深度对接区域产业对实战型人才的迫切需求，重点破解工业互联网、跨境数据流通等前沿领域的安全保障瓶颈，通过系统性构建“技术能力+合规意识+攻防实战”的培养体系，为筑牢大湾区数字生态防线提供核心人才支撑。此举既响应国家网络强国战略的使命要求，亦是赋能区域经济高质量发展、抢占全球数字竞争制高点的关键落子，亟需加速布局与实施。

5. 申请增设专业人才培养方案

《网络空间安全》本科专业人才培养方案

前言

为顺应数字化时代对网络安全人才的迫切需求,响应国家“网络强国”战略及“十四五” 规划中对网络安全的重点部署，本专业聚焦网络空间安全领域的核心知识与技能。通过深入分析行业发展趋势、权威就业报告（如麦可思研究院）以及来自网络安全企业的实际调研反馈，明确网络安全运维、渗透测试、安全防御与安全管理等领域具有强劲的发展潜力和人才缺口。本方案依据计算机类专业《普通高等学校本科专业类教学质量国家标准》《东软 TOPCARES 系列框架标准》等标准的相关要求制定。

本专业设计遵循 “教育创造学生价值” 的理念，借鉴 TOPCARES 一体化人才培养模式的精髓，以学生为中心，强调实践能力与应用技能的快速提升。通过项目驱动的学习方式和全过程质量保障，确保学员能够掌握应对现实网络安全威胁的实战能力，满足行业及区域经济发展对网络安全人才的急需，保障人才培养质量。

一、专业基本信息

专业名称：网络空间安全
专业代码：080911TK
所属院系：计算机学院

二、入学要求

本专业面向普通高级中学毕业招生，要求全日制普通高中毕业，理科生，英语语种考生。

凡符合高考报考条件和上述理科和语种要求者，均可通过参加高考并填写高考志愿表报考本专业。学校招生严格遵守教育部、各省招生办公室的有关政策和规定，遵循公平竞争、公正选拔、全面考核、综合评价的原则。在各有关省（区、市）招生委员会划定的录取最低控制分数线上，在保证完成招生计划的前提下，制定具体录取标准，进行择优录取。

三、学制与学位

基本学制：四年

修业年限： 3-8 年

授予学位： 工学学士学位

四、服务面向

本专业立足广东，面向粤港澳大湾区，主要培养如下高素质应用型专门人才：

（1）面向政府、事业单位、IT 类企业从事网络安全系统分析与方案设计、安全管理平台建设及实施、互联网应用系统安全保障等工作。

（2）面向政府、事业单位、IT 类企业从事云安全架构设计、数据加密与隐私保护服务、网络渗透测试与应急响应等相关工作。

（3）可继续攻读网络空间安全、网络工程及相关专业的硕士学位。

五、培养目标

本专业基于 OBE 教育理念，融合 TOPCARES 一体化人才培养框架，致力于培养德、智、体、美、劳全面发展，践行社会主义核心价值观，具备良好职业道德与人文素养的高素质应用型专门人才。学生需掌握扎实的数学与自然科学基础知识、计算机及网络空间安全核心理论，通过 TOPCARES 能力维度训练，形成网络安全系统规划设计、风险评估、数据隐私保护、渗透测试及应急响应等核心能力，具备社会责任感、创新思维、国际视野及较强实践能力，毕业后能胜任网络安全管理、安全系统运维、安全服务提供等领域工作，达成“技术知识与推理 + 实践应用 + 职业素养”的一体化培养成果。

本专业毕业生通过系统培养，5 年后应达成以下 TOPCARES 能力目标：

（1）践行职业伦理与社会责任感，以正确价值观为引领，在网络安全工作中展现高度责任心与合规意识，符合 TOPCARES 框架中“责任感与价值观”维度要求；

（2）具备开放式思维与创新能力，能运用 OBE 反向设计思维，独立分析并解决网络攻击防御、漏洞修复等复杂安全问题，形成“技术应用 + 问题解决”的综合能力；

（3）掌握跨团队协作与沟通技巧，在信息安全项目中能有效进行口头与书面表达，满足 TOPCARES“沟通与协作”能力标准；

（4）树立终身学习理念，通过自主学习持续掌握安全态势感知、新型防护技术等前沿知识，适应技术迭代与社会发展需求，达成 OBE 对“持续发展能力”的培养要求。

六、毕业要求（培养规格）

本专业旨在培养适应国家网络强国战略和产业发展需求的”应用技术型”网络空间安全人才。毕业要求对标国内工程教育专业认证标准，并结合中西部地区重点高校及行业特色制定，确保毕业生具备解决网络空间安全领域复杂工程问题的综合能力、扎实的实践技能与持续的职业发展潜力。毕业生应达到以下十二项核心能力要求：

1 技术知识与推理（Technical knowledge and reasoning)

能够运用自然科学、社会科学、人文科学及网络空间安全专业技术知识，对网络安全问题进行分析和解决。

1.1 相关科学知识

系统理解数学(如离散数学、概率论)、物理学、社会科学、人文科学及计算机科学的理论基础，并能将其用于网络空间安全领域相关问题的准确表述，如运用数学原理阐述密码学算法的安全性。

1.2 专业基础知识

能够将网络空间安全的基础理论知识(如密码学、网络安全、系统安全、应用安全)用于专业领域问题的抽象、分析与推演，包括安全威胁建模、安全架构设计、安全策略制定等。

1.3 专业知识

能够将网络空间安全专业知识与数学分析方法相结合，用于推演和分析专业领域内的复杂问题，如进行量化风险评估、攻击路径分析等。同时，能够将专业知识应用于网络安全解决方案的比较与综合，并能在方案中体现网络安全领域的新知识和新技术，如人工智能驱动的威胁检测、零信任安全架构等。

2 开放式思维与创新（Open thinking and innovation)

能够应用科学原理思考问题，运用系统思维、批判性思维和创造性思维对网络安全新问题进行分析和研究。

2.1 系统思维

能够运用系统观点，将网络安全视为由人、流程和技术构成的复杂系统，对各要素及其相互关系进行系统性认识，如设计和评估”纵深防御”体系的整体有效性。

2.2 批判性思维

能够针对网络空间安全领域的问题和现有解决方案提出疑问，从攻击者视角审视系统脆弱性，用有说服力的论证和推理对安全控制措施的有效性进行解释和判断。

2.3 创造性思维

能够通过主动性和创见性的思维，揭示网络攻击与防御的本质规律，并在此基础上产生新颖、独特的、具有应用价值的思维成果，如设计创新的防御策略或发现未知漏洞

(0-day)。

3 个人职业能力（Personal and professional skills)

具有较高的数字素养、自主学习和终身学习能力，能够按照”调研、设计、实施、归纳”的思路对网络安全问题进行分析推理，能使用现代工具对网络安全问题进行分析和模拟。

3.1 分析推理和解决问题的能力

能够运用相关理论、框架(如 NIST CSF、MITRE ATT&CK)和方法，识别、推理网络安全问题的关键环节，分析并寻求多种可替代的风险处置方案。

3.2 实验、调查和发现知识

能够根据研究对象特征，设计并执行渗透测试、漏洞评估、数字取证等实验方案；能够安全地开展实验，正确地采集日志、流量等数据，并对实验结果进行分析和解释，通过信息综合得到合理有效的结论。

3.3 数字素养

具备高度的数字安全意识和计算思维，遵循数字伦理规范，能利用丰富的数字化资源、专业的安全工具和攻防平台，主动抽象问题、分解问题、构造解决方案，开展探索和创新。

3.4 终身学习能力

能在网络安全技术和威胁模式快速演变的背景下，认识到自主和终身学习的必要性，具有自主学习的能力，能接受和应对新兴技术(如人工智能、物联网)带来的新挑战。

4 沟通表达与团队合作（Communication and teamwork)

在跨文化的背景下，能够就网络安全专业问题，以个人或团队的形式，通过口头表达、书面文档、视觉图表等与同行或社会公众进行沟通、交流、协作。

4.1 交流能力

能就网络安全领域的复杂技术问题，以口头汇报、技术报告、安全通告等多种方式，向技术人员、管理层等不同受众准确表达自己的观点，促进共识的达成。

4.2 团队合作

能够在多学科、多样性的团队(如安全运营中心(SOC) 、应急响应小组、DevSecOps 团队)中与其他成员进行有效地、包容性的沟通与合作。

5 态度与习惯（Attitude and manner)

具有积极的人生态度、良好的生活习惯和体美劳素养，能在专业实践中理解并遵守网络安全职业道德和规范。

5.1 个体性态度与习惯

具有积极的人生态度和良好的心理调适能力，尤其是在应对高强度的网络安全事件时能保持沉着冷静，养成良好的生活习惯和体美劳素养。

5.2 职业态度与习惯

具有热爱网络安全事业、实事求是的职业素养，严格遵守职业规范(如保密原则、授权测试原则)，坚持原则，诚实守信。

5.3 社会性态度与习惯

具有正确的社会性态度，文明礼貌，遵纪守法，特别是遵守《网络安全法》等相关法律法规。

6 责任感（Responsibility)

能够理解网络安全专业实践与社会的关联，在网络安全应用领域能够考虑公共健康与安全、可持续发展、关键基础设施保护、法律与伦理，以及社会与文化等制约因素。

6.1 对个体的责任感

明确个体在维护网络安全中的责任，能够自我认知、管理，通过持续学习实现个体成长。

6.2 对职业的责任感

恪守职业伦理，理解并遵守职业道德规范，尊重国家和国际通行的相关法律法规。

6.3 对社会的责任感

知晓和理解网络安全对国家安全、社会稳定和公众利益的重大意义，能够站在保护关键信息基础设施和社会可持续发展的角度思考专业实践，并能评估其可能对人类和环境造成的损害和隐患。

7 价值观（Ethical values)

践行社会主义核心价值观并实现价值观的自我认知，能够理解不同的价值观，具备一定的包容性，对价值问题的多样性进行识别、应用与评价。

7.1 个人价值观

树立远大理想，信念坚定，勤学修德，勇于担当维护国家网络安全的责任和使命，做到爱国、敬业、诚信、友善。

7.2 职业价值观

在网络安全专业实践中勤勉努力、诚实守信，能自觉履行对组织数据资产、用户隐私和公众福祉的保护责任。

7.3 社会价值观

践行社会主义核心价值观,真诚友善,理解个人行为与国家安全、社会稳定的关系。了解中国国情，坚持以爱国主义为核心的民族精神和以改革创新为核心的时代精神。

8 实践构思、设计、实现和运行为社会的贡献（Social contribution by application practice)

掌握面向网络空间安全领域全周期、全流程设计/开发解决方案的基本方法和技术，能够针对特定需求，完成单体和系统的构思、设计、实施和运行维护，并在多学科环境下，在设计开发解决方案的过程中，运用管理与经济决策方法。

8.1 外部的社会背景和自然环境

在网络安全专业实践过程中，理解安全措施(如数据监控、内容过滤)对社会、文化及个人隐私的影响，以及社会法律法规对网络安全实践的规范。

8.2 行业应用环境

熟悉网络安全行业的国际、国家及行业标准(如等级保护 2.0)，掌握行业典型工作规范；熟悉本行业相关的应用技术及其发展前景。

8.3 构思、系统工程方法和管理

掌握网络空间安全领域全周期、全流程的设计/开发解决方案的基本方法和技术，并能通过文献研究和威胁情报分析，寻求可替代的解决方案。

8.4 设计

能够针对特定需求，完成安全体系、安全策略或安全工具的设计，并在设计方案中运用风险管理与经济决策方法，体现创新意识。

8.5 实施

能按照网络安全项目的开发和部署周期进行过程管理,包括涉及不同学科交叉的多任务协调、时间进度控制、相关资源调度、人力资源配备等内容。

8.6 运行

能对安全运营(如事件响应、安全审计)的结果进行分析和解释，并通过信息综合得出合理有效的结论，以实现安全体系的持续改进。

8.7 创业意识与技能

能够将网络安全专业知识与商业知识有效结合,识别市场需求,探索将技术转化为具有商业价值或社会价值的产品或服务，兼具整合、创新和承担风险等特征。

七、TOPCARES 专业人才培养模式、专业特色与能力指标

（一）专业人才培养模式

本专业借鉴并深度融合了东软教育科技集团独创的 TOPCARES 一体化人才培养模式。该模式以成果导向教育(OBE)和 CDIO 工程教育理念为核心，秉持”教育创造学生价值”的宗旨，旨在培养学生的综合素养与核心竞争力。

1 TOPCARES 一体化培养：构建全维度能力体系

依托 TOPCARES“知识 - 能力 - 素养”一体化设计，实现四重融合：

（1）知识、能力与素质融合：将专业知识传授、实践技能训练与职业素养培育贯穿教学全程，助力德智体美劳全面发展；

（2）课程与项目融合：以“五级项目”为牵引，将理论课程与阶梯式实践项目深度绑定，形成“学练一体”的课程体系；

（3）课内与课外融合：延伸课堂至学科竞赛、技术社团、创新创业活动，构建全方位育人场景，落实“教、学、做”一体化；

（4）校企协同融合：打破校园与产业边界，将企业资源融入培养全流程，聚焦“专业能力 + 岗位适配”双提升。

2 产教深度协同：弥合理论与实践鸿沟

以 OBE“成果导向”为指引，通过四类举措实现教学与产业需求无缝衔接：

（1）共研培养方案：联合天融信、奇安信等头部企业，将行业前沿需求、技术标准与岗位能力要求融入教学大纲，确保内容贴近实战；

（2）共建潜心实训平台：打造“网络安全联合实验室”、“鹏城攻防实训靶场”，引入企业级设备与真实案例，提供沉浸式实践环境；

（3）项目驱动教学：拆解企业真实项目为教学任务，贯穿《网络攻击与防范》《Web安全》等核心课程，学生以团队形式完成全流程实践，强化复杂问题解决能力；

（4）以赛促学赋能：依托“KO 战队”、“星盾”等安全社团，系统组织 CTF 等竞赛，以竞赛检验成果、激发兴趣，锤炼技术实力与协作能力。

（二）专业特色

本专业依托 TOPCARES 框架，聚焦网络安全行业对“技术过硬 + 懂业务善管理”的复合型人才需求，构建“技术深耕 + 协同管理”双维度特色培养体系，塑造高素质复合型安全人才。

1 以技术硬实力为核心，筑牢专业立身之本

立足 TOPCARES“技术知识与实践应用”能力维度，构建分层递进的技术培养路径：

（1）阶梯式知识体系：从计算机基础（程序设计、网络等）到安全核心（密码学、协议分析等），再到方向深化（漏洞挖掘、Web 安全等），形成“基础 - 核心 - 应用”完整知识链；

（2）实战化能力锻造：通过课程实验、综合实训及 Capstone 毕业设计，强化安全

工具操作、安全软件开发能力，要求学生以真实复杂安全问题为导向完成毕业设计，全面检验技术整合能力；

（3）安全思维塑造：以“攻击者视角”贯穿教学，通过攻防演练与案例分析，训练学生系统分析安全问题、推理攻击路径、设计防御策略的底层思维，实现从“会操作”到“能创造”的跃升。

2 以协同管理素养为支撑，培育行业骨干潜力

紧扣 TOPCARES“职业素养与协作能力”培养要求，聚焦安全工作的协同属性：

（1）简易化项目协作训练：在课程实践中融入小型团队任务（如 2-3 人小组完成安全工具配置、简单漏洞扫描等），嵌入基础协作要素（如任务分工表、进度跟踪表），让学生掌握团队作业的基本流程，提升任务执行力；

（2）小规模团队协作实践：以课程设计、小型竞赛项目为载体（每组 3-5 人），模拟企业基层团队场景，重点训练任务拆解、信息同步、简单冲突协调等基础能力，确保学生能快速融入职场团队；

（3）实用化沟通与责任意识培养：强化 “技术表达基本功”，训练学生清晰撰写实验报告、项目小结，能在团队中简明阐述技术思路；结合网络安全法基础条款、典型违规案例，培育学生遵守行业规范的责任意识，避免技术滥用，形成符合一线岗位要求的职业行为习惯。

通过双维度融合，实现“技术专精 + 管理协同”的差异化培养，契合行业对复合型安全人才的核心需求。

（三）专业人才培养能力指标

TOPCARES（一级指标）	TOPCARES（二级指标）	TOPCARES（三级指标）
1 Technical knowledge and reasoning 技术知识与推理	1.1 相关科学知识	1.1.1 人文社会科学知识
		1.1.2 数学与自然科学知识
		1.1.3 外语知识
	1.2 专业基础知识	1.2.1 专业基础知识
	1.3 专业知识	1.3.1 专业核心知识、方法和工具
2 Open thinking and innovation 开放式思维与创新	2.1 系统思维	2.1.1 整体性思维
		2.1.2 系统的显现和交互作用
	2.2 批判性思维	2.2.1 分析问题
		2.2.3 选择逻辑论点和解决方法
	2.3 创造性思维	2.3.6 引进、消化、吸收再创新能力
	3.1 分析推理和解决问题的能力	3.1.1 发现问题和表述问题
		3.1.7 解决方法和建议

TOPCARES（一级指标）	TOPCARES（二级指标）	TOPCARES（三级指标）
3 Personal and professional skills 个人职业能力	3.2 实验、调查和发现知识	3.2.2 查询印刷资料和电子文献
	3.3 数字素养	3.3.3 数据、信息和数字内容的获取、分析、应用
	3.4 终身学习能力	3.4.1 终身学习的态度（求知欲、主动性...）
		3.4.2 终身学习的技能（自主学习、迁移、反思...）
4 Communication and teamwork 沟通表达与团队合作	4.1 交流能力	4.1.3 阅读与理解
		4.1.4 书面交流
		4.1.7 口头表达
		4.1.8 使用外语能力（基本交流能力、专业交流能力）
	4.2 团队合作	4.2.1 团队合作（团队组建、运行、成长和演变）
5 Attitude and manner 态度与习惯	5.1 个体性态度与习惯	5.1.1 健康生活（体育素养）
		5.1.3 实践创新（劳动素养）
	5.2 职业态度与习惯	5.2.1 热爱事业
		5.2.3 实事求是
	5.3 社会性态度与习惯	5.3.1 文明礼貌
		5.3.2 爱护环境
		5.3.3 遵纪守法
6 Responsibility 责任感	6.1 对个体的责任感	6.1.2 自我管理
	6.2 对职业的责任感	6.2.2 职业行为
	6.3 对社会的责任感	6.3.1 社会责任
		6.3.2 国家认同
7 Ethical values 价值观	7.1 个人价值观	7.1.1 理想信念（理想远大、信念坚定）
		7.1.2 价值养成（勤学修德、明辨笃实）
	7.2 职业价值观	7.2.1 敬业乐群（勤勉努力、克己奉公）
		7.2.2 诚实守信（真实诚恳、信守承诺）
	7.3 社会价值观	7.3.1 爱国主义（爱国、爱党、爱社会）
8 Social contribution by application practice 实践构思、设计、实现和运行为社会的贡献	8.1 外部的社会背景和自然环境	8.1.1 工程（复杂问题解决方案）对社会和自然环境的影响
	8.2 行业应用环境	8.2.1 行业的基本规范
		8.2.2 行业应用技术
	8.3 构思、系统工程方法和管理	8.3.4 开发项目的管理
	8.4 设计	8.4.1 设计过程
	8.5 实施	8.5.1 设计可持续的实施过程
	8.6 运行	8.6.4 系统改进和演变

TOPCARES（一级指标）	TOPCARES（二级指标）	TOPCARES（三级指标）
	8.7 创业意识与技能	8.7.1 创业意识（发现、观念发展、资源整合、付诸实践...）
		8.7.2 创业技能（财务管理、人力资源管理、营销管理、运营管理、战略管理、风险管理、知识产权管理...）

八、毕业学分要求

本专业学生毕业时应达到学校对本科生提出的德智体美劳全面发展的要求，总修读学分不少于 179.5 学分。大学生体质健康测试成绩须达 50 分。各类课程应修最低学分见下表：

课程结构	学分要求			
	必修	专业选修	通识选修	合计
通识课程	65.5		8	73.5
学科及专业基础课程	44			44
专业课程	17	15		32
集中实践环节	30			30
合计	156.5	15	8	179.5

备注：创新创业及素质教育类课程包含在通识课程中。其中创新创业必修课程 4 学分，创新创业及素质教育实践要求 1 学分，创新创业通识选修课程 2 学分，共计 7 学分。

九、课程设置及学时学分安排

（一）专业核心课程设置

序号	课程代码	课程名称	学时	学期	备注
1	CS3255	程序设计基础	80	1	
2	CS3281	数据结构与算法	80	2	
3	CS3013	操作系统原理	64	5	
4	CS3018	计算机网络	64	4	
5	CS3284	数据库系统原理	64	4	
6	CS3591	密码学与网络安全	48	5	
7	CS3745	Web 安全技术	48	5	

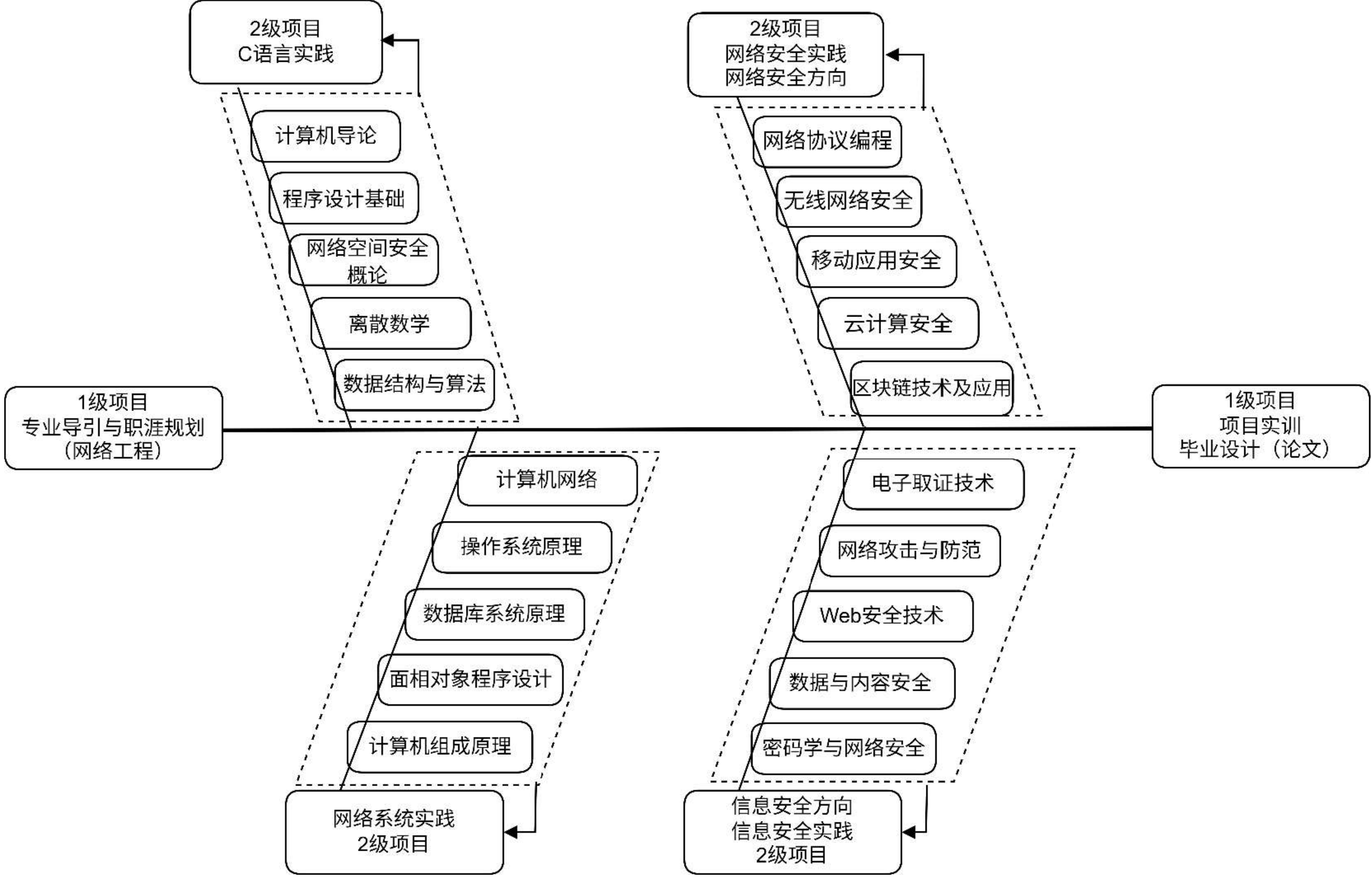
8	CS3283	计算机组成原理	48	5	
9	CS3350	软件系统安全	64	8	
10	CS3295	网络攻击与防范	64	7	

（二）专业项目设置

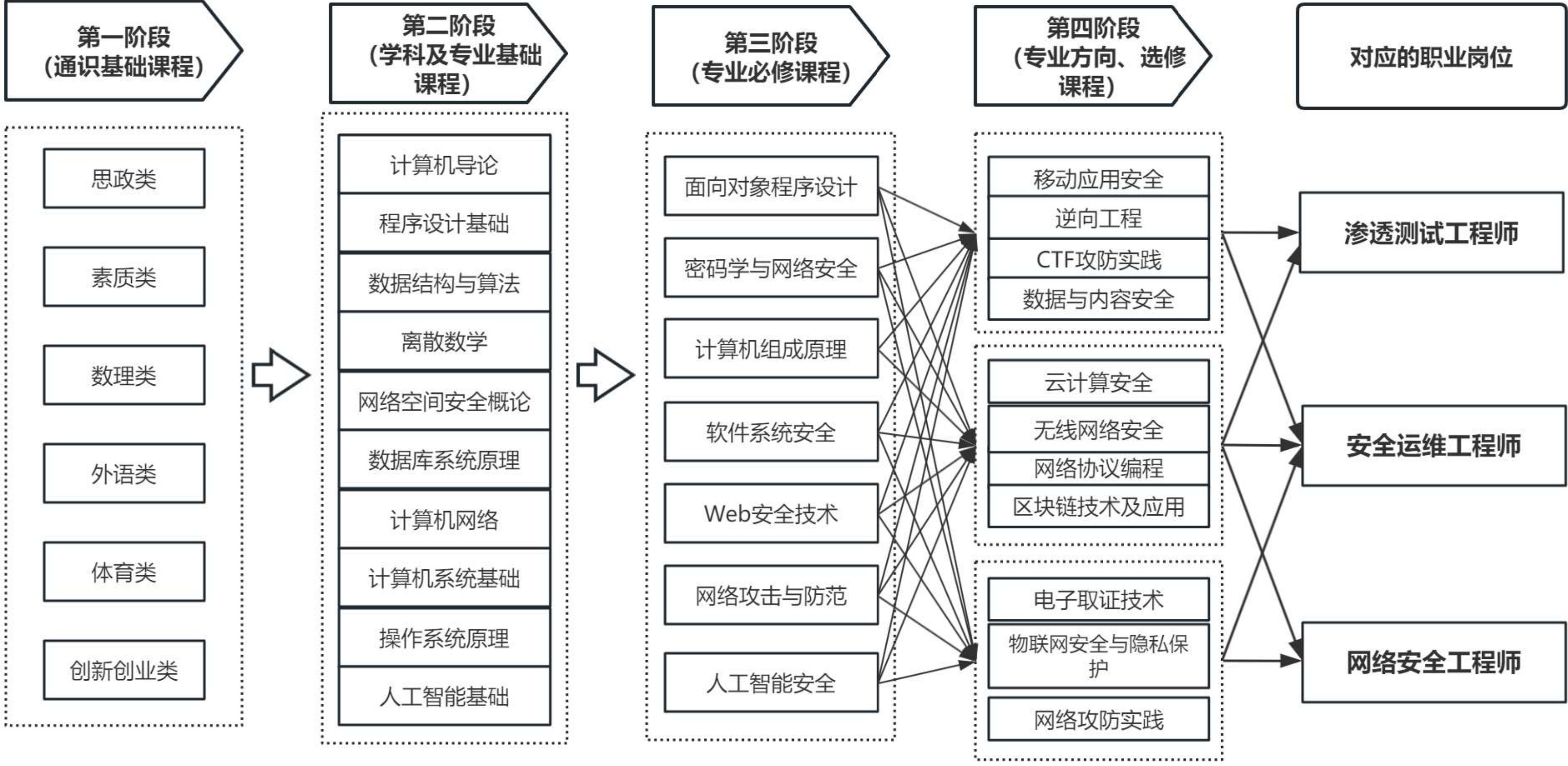
序号	项目等级	项目代码	项目名称	学分	学期	对应主要课程名称
1	一	PCS31009	专业导引与职涯规划（网络空间安全）	1	1	网络空间安全导论
2	三	PCS33005	程序设计基础课程设计	0.5	1	程序设计基础
3	三	PCS33006	数据结构与算法课程设计	0.5	2	数据结构与算法
4	二	PCS32033	程序设计实践	4	3	程序设计基础/数据结构与算法
5	二	PCS32034	网络系统实践	4	6	数据库系统原理/操作系统原理/计算机网络/Web编程技术/面向对象程序设计
6	二	PCS32036	网络安全实践	4	9	密码学与网络安全/Web安全技术/网络攻击与防范/电子取证技术
7	一	PCS31010	项目实训	8	10	专业相关课程
8	一	PCS31020	毕业设计	8	11	专业相关课程

备注：只填写本专业一、二级项目和单独设置学分的三级项目。

（三）项目导向的专业课程能力培养鱼骨图



（四）课程设置与主要职业岗位对应关系链路图



（五）培养计划课程设置进程表

课程类别			课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
								理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
												1	2	3	4	5	6	7	8	9	10	11		
通识课程平台	通识必修课程模块	思政类	GE6267	思想道德与法治	必修	2.5	40	40				2.5											马克思主义学院	必修65.5学分
			GE6273	中国近现代史纲要	必修	2.5	40	40					2.5										马克思主义学院	
			GE6275	马克思主义基本原理	必修	2.5	40	40							2.5								马克思主义学院	
			GE6307	毛泽东思想和中国特色社会主义理论体系概论	必修	2.5	40	40								2.5							马克思主义学院	
			GE6308	习近平新时代中国特色社会主义思想概论	必修	2.5	40	40								2.5							马克思主义学院	
			GE6339	思政实践 I	必修	0.5	8		8			0.5											马克思主义学院	
			GE6340	思政实践 II	必修	0.5	8		8				0.5										马克思主义学院	
			GE6341	思政实践 III	必修	0.5	8		8						0.5								马克思主义学院	
			GE6342	思政实践 IV	必修	0.5	8		8							0.5							马克思主义学院	
			GE6343	思政实践 V	必修	0.5	8		8							0.5							马克思主义学院	
			GE6225	马克思主义中国化进程与青年学生使命担当	必修	1	24	24				1											马克思主义学院	
			GE6175	形势与政策Ⅰ	必修	0.25	8	8				0.25											马克思主义学院	

课程类别	课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
						理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
										1	2	3	4	5	6	7	8	9	10	11		
	GE6176	形势与政策Ⅱ	必修	0.25	8	8					0.25										马克思主义学院	
	GE6177	形势与政策Ⅲ	必修	0.25	8	8							0.25								马克思主义学院	
	GE6178	形势与政策Ⅳ	必修	0.25	8	8								0.25							马克思主义学院	
	GE6179	形势与政策Ⅴ	必修	0.25	8	8										0.25					马克思主义学院	
	GE6180	形势与政策Ⅵ	必修	0.25	8	8											0.25				马克思主义学院	
	GE6181	形势与政策Ⅶ	必修	0.25	8	8													0.25		马克思主义学院	
	GE6182	形势与政策Ⅷ	必修	0.25	8	8														0.25	马克思主义学院	
	GE6436	国家安全教育	必修	1	16	12	4			1											马克思主义学院	
素质类	GE6272	劳动教育	必修	0.5	10	8	2			0.5											基础教学院	
	GE6023	大学生心理健康教育	必修	2	32	26	6			2											学生工作部	
	GE6293	实验室安全教育	必修	0	2	2				√											实验实训中心	
	GE6294	社会实践	必修	1	16	2			14		1										马克思主义学院	

课程类别	课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
						理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
										1	2	3	4	5	6	7	8	9	10	11		
	GE6197	大学生就业指导	必修	1	16	16										1					马克思主义学院	
外语类	GE6220	大学英语Ⅰ	必修	3	48	48				3											外国语学院	
	GE6229	大学英语Ⅱ	必修	3	48	48					3										外国语学院	
	GE6437	大学英语Ⅲ	必修	2	32	32							2								外国语学院	
	GE6421	理工应用英语	必修	2	32	32								2							外国语学院	
数理类	GE6173	高等数学Ⅰ（理工类）	必修	6	96	96				6											基础教学院	
	GE6045	高等数学Ⅱ（理工类）	必修	4	64	64					4										基础教学院	
	GE6001	线性代数	必修	3	48	48							3								基础教学院	
	GE6009	概率论与数理统计	必修	3	48	48								3							基础教学院	
	GE6246	大学物理	必修	4	64	64					4										基础教学院	
	GE6292	大学物理实验	必修	1	24			24					1								基础教学院	
体育	GE6219	军事理论	必修	2	36	36					2										基础教学院	

课程类别			课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
								理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
												1	2	3	4	5	6	7	8	9	10	11		
		类	GE6187	体育Ⅰ	必修	1	36		36			1											基础教学院	
			GE6188	体育Ⅱ	必修	1	36		36				1										基础教学院	
			GE6189	体育Ⅲ	必修	0.5	18		18						0.5								基础教学院	
			GE6190	体育Ⅳ	必修	0.5	18		18							0.5							基础教学院	
			GE6191	体育Ⅴ	必修	0.5	18		18									0.5					基础教学院	
			GE6192	体育Ⅵ	必修	0.5	18		18										0.5				基础教学院	
		创新创业类	GE6309	创新、创造与改变	必修	1	32	14	18			1											创新创业学院/SOVO	
			GE6310	思维创新与开发	必修	1	32	16	16				1										创新创业学院/SOVO	
			GE6311	创业者的成长之路	必修	1	32	24	8						1								创新创业学院/SOVO	
			GE6312	从非商业计划到商业计划	必修	1	32	16	16							1							创新创业学院/SOVO	

课程类别		课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
							理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
											1	2	3	4	5	6	7	8	9	10	11		
		GE6295	创新创业及素质教育实践	必修	1																	计算机学院	
应修小计					65.5	1232	940	254	24	14	18.75	19.25	0	10.75	12.75	0	1.75	0.75	0	0.25	0.25		
通识选修课程模块	人文社科类		详见通识选修课程库	选修	2	32	32				最低学分要求 8 学分，人文社科类、自然与科技类、创新创业类、艺术类四类课程每类至少修 2 学分。												通识选修 8 学分
	自然与科技类		详见通识选修课程库	选修	2	32	32																
	创新创业类		详见通识选修课程库	选修	2	32	32																
	艺术类		详见通识选修课程库	选修	2	32	32																
应修小计					8	128	128							2	2		2	2					
学科及专业基础课程平	学科基础课程模块	CS3421	计算机导论	必修	2	32	32				2											计算机学院	必修 44 学分
		CS3255	程序设计基础★	必修	5	80	56		24		5											计算机学院	
		CS3318	程序设计基础课程设计	必修	0.5	16		16			0.5											计算机学院	
		CS3281	数据结构与算法★	必修	5	80	56		24			5										计算机学院	
		CS3336	数据结构与算法课程设计	必修	0.5	16		16				0.5										计算机学院	

课程类别		课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
							理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
											1	2	3	4	5	6	7	8	9	10	11		
台		CS3041	离散数学	必修	4	64	64		0		4											计算机学院	
		CS3013	操作系统原理★	必修	4	64	48		16						4							计算机学院	
		CS3018	计算机网络★	必修	4	64	48		16						4							计算机学院	
	专业基础课程模块	CS3679	计算机组成原理	必修	3	48	32		16			3										计算机学院	
		CS3363	数据库系统原理	必修	3	48	32		16					3								计算机学院	
		CS3369	网络空间安全概论	必修	3	48	48							3								计算机学院	
		CS3350	计算机系统基础★	必修	4	64	48		16						4							计算机学院	
		CS3678	人工智能基础	必修	3	48	32		16								3						
		CS3677	面向对象程序设计	必修	3	48	32		16					3								计算机学院	
	应修小计				44	624	464	32	128		11.5	8.5		9	12		3						
专业课程平	专业必修课程模块	CS3572	专业导引与职涯规划（网络空间安全）	必修	1	16		16			1											计算机学院	必修17学分
		CS3690	人工智能安全	必修	4	64	48		16									4				计算机学院	
		CS3285	密码学与网络安全★	必修	3	48	40		8						3							计算机学	

课程类别		课程代码	课程名称	课程性质	学分	总学时	课内学时 理论授课	课内实践	实验室实验	课外学时	第一学年 1	2	3	第二学年 4	5	6	第三学年 7	8	9	第四学年 10	11	开课单位	学分要求
台																						院	
		CS3295	网络攻击与防范	必修	3	48	32		16								3					计算机学院	
		CS3299	软件系统安全	必修	3	48	48											3				计算机学院	
		CS3293	Web 安全技术	必修	3	48	32		16						3							计算机学院	
应修小计					17	176	120	16	40		1			0	6		3	7					
专业选修课程模块	网络安全方向	CS3496	网络协议编程	选修	3	48	32		16									3				计算机学院	专业选修15学分其中：第7学期8学分第8
		CS3376	无线网络安全	选修	2	32	24		8								2					计算机学院	
		CS3292	移动应用安全	选修	2	32	24		8								2					计算机学院	
	信息安全方向	CS3296	电子取证技术	选修	2	32	24		8								2					计算机学院	
		CS3386	数据与内容安全	选修	3	48	32		16									3				计算机学院	
		CS3382	逆向工程	选修	2	32	24		8								2					计算机学院	
	专业任	CS3500	区块链技术及应用	选修	2	32	24		8									2				计算机学院	
		CS3689	云计算安全	选修	2	32	24		8									2				计算机学	

课程类别		课程代码	课程名称	课程性质	学分	总学时	课内学时：理论授课	课内学时：课内实践	课内学时：实验室实验	课外学时	第一学年 1	2	3	第二学年 4	5	6	第三学年 7	8	9	第四学年 10	11	开课单位	学分要求
	选课																					院	学期7学分
		CS3705	网络攻防实践	选修	2	32	16		16									2				计算机学院	
		CS3399	CTF 攻防实践	选修	2	32	16		16								2					计算机学院	
		CS3707	物联网安全与隐私保护	选修	2	32	24		8									2				计算机学院	
		CS3709	网络安全程序设计	选修	2	32	24		8								2					计算机学院	
		CS3735	网络工程师认证	选修	2	32	24		8								2					计算机学院	
		CS3765	程序分析与安全	选修	2	32	24		8								2					计算机学院	
	应修小计				15	240	180	0	60								8	7					
集中实践环节	军训类	GE6251	军事技能	必修	2	2周		2周			2											学生工作部	必修30学分
	专业实践（实训）类	CS3564	基本能力实训	必修	4	4周		4周					4									计算机学院	
		CS3565	专业能力实训	必修	4	4周		4周								4						计算机学院	
		CS3566	综合能力实训	必修	4	4周		4周											4			计算机学院	

课程类别	课程代码	课程名称	课程性质	学分	总学时	课内学时			课外学时	学期											开课单位	学分要求
						理论授课	课内实践	实验室实验		第一学年			第二学年			第三学年			第四学年			
										1	2	3	4	5	6	7	8	9	10	11		
	CS3452	项目实训	必修	8	8周		8周												8		计算机学院	
毕业设计类	CS3457	毕业设计（论文）	必修	8	16周		16周													8	计算机学院	
应修小计				30	832		832			2		4			4			4	8	8		
合计				179.5	3232	1832	1134	252	14	33.25	27.75	4	21.75	32.75	4	17.75	16.75	4	8.25	8.25		

（六）实践教育教学环节

主要包括实验、实训、实习、企业项目开发实训、证书、创新创业及素质教育实践，社会实践、毕业设计（论文/毕业作品）等，并将劳动教育融入各类型实践教学环节。

劳动教育由 3 部分组成，分别是课程劳育、实践劳育和专业劳育，共计 32 学时。

（1）课程劳育：课设《劳动教育》课程，其中理论教学 8 学时，课内实践 2 学时；

（2）实践劳育：穿插于素质教育活动，不少于 10 学时；

（3）专业劳育：穿插于专业课程、实习、实训教学，不少于 12 学时。

1．课程实验教学进程表

序号	开设学期	课程代码	课程名称	实验学时
1	1	CS3255	程序设计基础	24
2	1	CS3318	程序设计基础课程设计	16
3	2	CS3281	数据结构与算法	24
4	2	CS3336	数据结构与算法课程设计	16
5	4	CS3363	数据库系统原理	16
6	4	GE6292	大学物理实验	24
7	4	CS3018	计算机网络	16
8	4	CS3350	计算机系统基础	16
9	5	CS3679	CTF 攻防实践	16
10	5	CS3591	密码学与网络安全	8
11	5	CS3013	网络攻防实践	16
12	7	CS3678	人工智能基础	16
合计				208

2．集中实践环节教学进程表

序号	环节类别	集中实践环节名称	学分	周数	学期	备注
1	军训类	军事技能	2	2	1	
2	专业实践（实训）类	基本能力实训	4	4	3	
3	专业实践（实训）类	专业能力实训	4	4	6	
4	专业实践（实训）类	综合能力实训	4	4	9	
5	专业实践（实训）类	项目实训	8	8	10	
6	毕业设计类	毕业设计（论文）	8	16	11	
合计			30	38		

3．创新创业及素质教育实践学分

创新创业及素质教育项目主要包括创新创业项目、专业认证和素质教育项目共三类。其中，各专业重点推荐学生选修的项目如下：

序号	项目级别	项目名称	学分	重要活动标“*”	备注
1	校级	中国“互联网+”大学生创新创业大赛	2	*	省级三等奖以上
2	校级	“挑战杯”全国大学生课外学术科技作品竞赛和创业计划大赛	2	*	省级三等奖以上
3	校级	全国大学生数学建模竞赛	2	*	省级三等奖以上
4	校级	中国高校计算机大赛	2	*	省级三等奖以上
5	校级	全国大学生计算机系统能力培养大赛	2	*	省级三等奖以上
6	校级	全国大学生电子设计竞赛	2	*	省级三等奖以上
7	校级	中国大学生计算机设计大赛	2	*	省级三等奖以上
8	校级	ACM 国际大学生程序设计竞赛	2	*	省级三等奖以上
9	校级	CCF 大学生计算机系统与程序设计竞赛	2	*	省级三等奖以上
10	校级	蓝桥杯全国软件和信息技术专业人才大赛	1	*	省级三等奖以上
11	校级	华为 ICT 大赛	1	*	省级三等奖以上
12	校级	C4-网络技术挑战赛	1	*	省级三等奖以上
13	校级	国家级大学生创新创业训练计划	1.5	*	获得立项
14	校级	国家级大学生创新创业训练计划	0.5	*	获得结题
15	校级	省级大学生创新创业训练计划	1	*	获得立项
16	校级	省级大学生创新创业训练计划	0.5	*	获得结题
17	校级	“攀登计划”广东大学生科技创新培育项目	1.5	*	获得立项
18	校级	“攀登计划”广东大学生科技创新培育项目	0.5	*	获得结题
19	校级	计算机技术与软件专业技术资格（水平）考试	2		获得高级证书
20	校级	计算机技术与软件专业技术资格（水平）考试	2		获得中级证书
21	校级	计算机技术与软件专业技术资格（水平）考试	1		获得初级证书
22	院级	实践学期作品竞赛	1		获得一等奖
23	院级	实践学期作品竞赛	0.5		获得二等奖
24	院级	实践学期作品竞赛	0.3		获得三等奖
25	院级	程序设计竞赛	1		获得一等奖

序号	项目级别	项目名称	学分	重要活动标“*”	备注
26	院级	程序设计竞赛	0.5		获得二等奖
27	院级	程序设计竞赛	0.3		获得三等奖
28	院级	计算机设计大赛	1		获得一等奖
29	院级	计算机设计大赛	0.5		获得二等奖
30	院级	计算机设计大赛	0.3		获得三等奖
31	院级	计算机设计大赛	1		获得一等奖

备注：

1. 素质教育项目级别分为校级、院级（专业群级）、系级。
2. 素质教育项目的选取要切实结合专业培养目标和毕业要求，突出专业特色。
3. 学生毕业前必须完成 1 学分的创新创业及素质教育实践学分。

（七）各类课程学时学分统计表

课程类别	必修课：　156.5 学分							选修课：23 学分			实践学分	总学分
	通识必修课		学科及专业基础课		专业课		集中实践环节	通识选修课	专业选修课			
	理论	实践	理论	实践	理论	实践	实践	理论	理论	实践		
学分	53.59	11.91	30.50	10.50	13.50	6.50	30.0	8.0	11.25	3.75	62.66	179.5

实践教学环节学分所占比例：34.91%

课程类别	必修课							选修课			实践学时	总学时
	通识必修课		学科及专业基础课		专业课		集中实践环节	通识选修课	专业选修课			
	理论	实践	理论	实践	理论	实践	实践	理论	理论	实践		
学时	940	292	464	160	120	56	38 周	128	180	60	1386	3232

实践教学环节学时所占比例：42.88%

备注：

1．集中实践教学环节中军训类、专业实践（实训）类每 1 周计 1 学分，毕业设计（论文）每 2 周计 1 学分。

2．实践教学环节学时所占比例=各类课程实践学时之和/总学时。

3．集中性实践教学环节其中《军事技能》按 8 学时/天计算，其他课程每周折算 20 学时，实践学时=总学时-理论授课学时。

4．创新创业及素质教育学时只计算创新创业课程的学时，创新创业及素质教育实践学分不折算学时。

5．专业选修课理论（实践）学时=（专业选修课最低要求学分/计划中列出的专业选修课学分之和）×专业选修课理论（实践）学时之和。

6．通识选修课的学时=通识选修课的学分要求×16，全部计入理论学时。

7．通识必修课单门课课程学分计算公式如下：

单门课理论学分=该课程理论教学学时/该课程总学时×该课程总学分；

单门课实践学分=该课程实践教学学时/该课程总学时×该课程总学分。

（八）本专业混合式教育实施计划

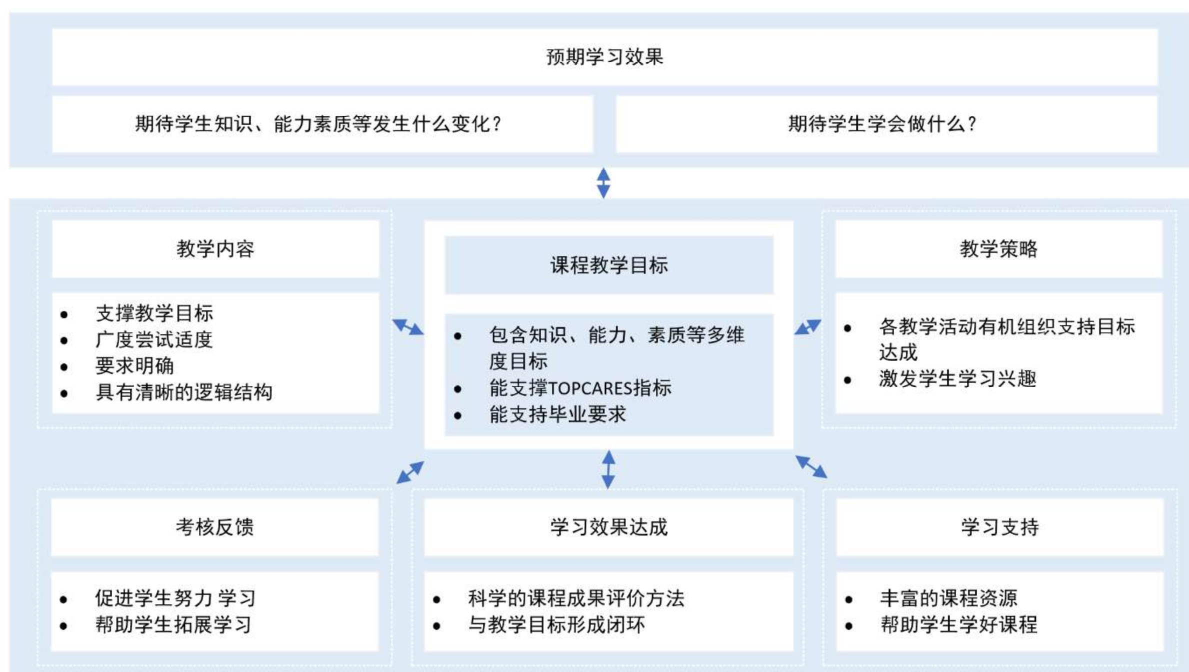
1. 持续丰富拓展 TOPCARES 方法学内涵，深化混合式教育模式变革

以学生为中心，产出为导向，融合学校文化与专业特色，构建混合式教学生态系统，创新教育教学模式。聚焦课程建设，作为教学质量提升的关键，强化设计、技术、资源与质量评价，持续优化混合式教育模式，追求更高教育成效与产出。



2. 以学生为中心，注重混合式教学课程设计

聚焦于“助学生高效学习”的教学设计，通过问题情境、活动、交互及资源，促进个性化学习达成。目标设计上超越知识点，挖掘背后的方法、思维与能力，聚焦核心能力培养。课程设计整合前期开发与学习支持，视为整体。建设过程中考虑自主学习与时空分离挑战，设计精准学习支架，如活动步骤、资源工具等，以科学化设计推动混合式教学改革。



十、教学基本条件

（一）师资队伍

1．专业带头人的基本要求

专业带头人应具有副教授及以上职称，并在具有网络空间安全、计算机或相关专业上具有深厚的学术造诣，能带领网络空间安全专业教师团队进行专业建设。应主持或作为主要参与人参与过网络空间安全专业人才培养方案的制定或修订工作。要求定期参加国内外网络空间安全及教育技术相关会议，能将网络空间安全专业的最新教育教学成果与学校及本专业发展相结合，熟悉教育规律，能制定并实施专业建设规划。此外，专业带头人还应在科研方面有所建树，发表过高水平学术论文，保持持续的科研活动，对网络空间安全领域的最新研究动态有深入了解。有主持或参与省级以上科研项目的经历，能够将科研成果转化为教学资源，促进教学质量和学术水平的提升。积极推动科研与教学相结合，鼓励和支持团队成员参与科研项目，形成一只老中青结构合理的创新团队，提升整个教学团队的科研能力。

2．专任教师与兼职教师的配置与要求

（1）网络空间安全专业教师队伍的规模应满足专业发展的需要。专任教师总数一般应使生师比不高于24:1，兼任教师人数应当不超过本专业专任教师总数的20%，，形成“专任主教、兼职主训”的协同模式。

（2）教师应具备的网络空间安全（行业）从业资格和任职经历需满足网络空间安全应用型人才培养需要。专任教师应具有研究生学历及以上；获得 CISP-PTE、CCIE-Sec 等行业资格认证的主讲教师比例应不低于专任教师总数的50%。

（3）网络空间安全专业的教师队伍中，具有 2 年以上网络相关企业工作经历或工程背景的教师比例应不低于50%。

（4）企业兼职教师一般应为资深网络工程师或具有同等水平的专业技术人员，且具有3-5年或以上网络空间安全相关工作经验。

3．专业核心课程及项目建设团队的配置和要求

（1）专业基础课，涵盖程序设计基础、数据结构与算法、操作系统原理、计算机网络、计算机系统基础等，这些课程是构建专业知识体系的基石。该类课程共需教师 10 人，其中高级职称教师占比需达到 30% 以上，具备工程经验的教师占比也需在 30% 以上，以保障基础教学的专业性与实用性；

（2）专业课，包含数据库系统原理、密码学与网络安全、Web 安全技术、Web 编程技术、网络攻击与防范等核心课程。每门课程需配备 2 名教师，此类课程共需教师 14 人，且要求具备工程经验的教师占比不低于 50%，确保学生能接触到贴合实际应用的专业知识与技能；

（3）实践与实训类课程，基于上述专业基础课和专业课的实践环节设置，旨在提升学生的动手能力与解决实际问题的能力。该类课程需教师 10 人，其中具备工程经验的教师占比需达到 50% 以上，以更好地指导学生开展实践训练。

（二）教学设施

1．专业教室应达到的基本条件

本专业所有课程都要求在多媒体教室讲授，多媒体教室需配备先进的投影仪、音响系统，以及教师端和所有学生的网络接口，支持网络教学与实验演示。

2．校内实验及实训基地的基本要求

校内实验及实训基地主要为网络空间安全专业培养方案课程体系中的实践教学环节提供支持，应能满足网络空间安全课程实验对软硬件设备的需求，同时，为了孵化学生创新性实验训练计划项目，为学生参加各级各类网络空间安全实践竞赛提供质量保障。因此，实验室的硬件资源以及配套的软件资源需要不断更新，保持与行业同步。

3．校外实习及实训基地的基本要求

校外实习及实训基地应能够承担专业的部分实践教学任务，能接受一定数量的教师与学生开展实习实训。实习实训基地应按照网络空间安全专业人才培养方案的要求提供实习实训项目和指导教师，并能满足实习学生在实习期间的学习、劳动保护和酬金等方面的条件。

（三）教学资源

1．教材选用的基本要求

（1）教材选取要求

教材选用应结合网络空间安全专业应用型人才培养的要求，内容须符合《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》等国家法律法规，无境外敌对站点、工具或案例引用。教材选用应根据课程在网络空间安全专业培养方案中的地位和作用，课程的教学基本要求和教学大纲，同时要考虑教学模式、教学方法和学生的实际情况，优先选择适用于学校应用型人才培养的教材，合理选用我校自编的 TOPCARES 教材、近三年内出版的优秀教材、国家教育部及省级规划教材、业界公认的优秀教材及国外优秀网络空间安全教材等。在教材选用过程中，要求每门课程至少比较分析 5 本国内外同类教材后方可推荐使用，在比较分析时要给出具体推荐理由和相应依据，做到覆盖课程全部知识点，配备实验指导书、源代码、在线靶场、习题库及微课视频。

（2）教案与课件编写要求

①每门课程要有完整的教案和课件，并且经过课程组讨论后，由主管教学副主任批准后方可使用。

②课件编写的原则是适合内容、利于教学。建议采用但不限于 PPT 文档，其内容应包含较为完整的知识体系，但不宜出现大篇幅文字，应结合课程特点，以知识点总结、图表举例、动画演示等多种形式，补充不宜体现在教材的静态文本中的内容。

③教案应根据课程标准、教学大纲和教科书要求及学生的实际情况，以课时或课题为单位，对教学内容、教学步骤、教学方法等进行设计，达到有效地组织教学活动的目的。

④教案应包括教学总结，对当堂课的一系列教学活动进行评价，明确教学方法、教学内容等方面存在的问题，并每学期依据护网新漏洞、学生反馈、督导数据提出解决方法，形成持续改进。

（3）题库、案例库、项目库等资源建设要求

① 每门课程（包括实践学期的二级项目以及实训的一级项目）都至少要有一定量的题库、案例库或者项目库。

② 题库、案例库、项目库内容要结合课程特点定期更新，一方面要根据业界主流技术的变化增加新应用、新工具、新产品、新方法等内容，另一方面要淘汰过时的资源，变化不大的课程（如原理性课程）也要定期更新题目的类型、描述等信息，避免多届学生使用相同资源库。根据实际情况建议每年更新比例不低于 10%。

③ 题库建设要能够支持教考分离对数目、质量等方面的需求。

2．信息化资源配备的基本要求

充分使用各种信息化教学平台和系统，提升工作效率，提升教学质量。建议至少充分使用以下信息化平台：

（1）信息化资源主要包括：各种教学用网站和考试系统，如视频信息管理系统、资源复用教学支持平台、万维考试系统等；

（2）专业教学资源：各门课程的课件、教案、题库、案例库、项目库、网络靶场、安全防护等；

（3）课程学习资源：互联网中的 MOOC、公开课资源，Kali、Metasploitable、DVWA、VulnHub、区块链靶机等；

（4）开放式学习平台：作业管理系统、MOOC 平台等；

（5）创新创业平台：学校创新实践云平台、大学生创新创业管理平台等同时实现专业信息化资源与校园教育教学资源的共享和一体化的管理，支持专业人才培养目标和发展计划，支持专业柔性学习体系的建设，保持专业良性发展。

十一、质量保障

建立以提高教育教学质量为导向的管理制度和工作机制，以服务为宗旨，以就业为

导向，把教育资源配置和工作重点集中到强化教学环节，并对思政教育的设计和实施提供有效的支持和保障。针对网络空间安全专业，质量保障具体措施如下：

1．教师知识技能持续提升机制

（1）课程组每周至少进行一次集体备课，课程群每月至少进行一次教学研讨。

（2）组织教师参加学校、系部和团队组织的公开课，学习优秀教师的授课经验。

（3）鼓励并支持教师参与国内外网络空间安全相关的学术会议、研讨会，以及在线教育技术培训，提升教学与研究能力。

（4）实施“导师制”，为新入职教师配备经验丰富的导师，加速其教学技能和专业成长。

2．教学活动监控机制

（1）根据学校《广东东软学院TOPCARES模式本科教学主要环节质量标准》对混合式教学改革主要环节进行质量监控。

（2）根据学校《学校 TOPCARES 模式课程/项目资源建设要求和技术规范》对课程和项目建设的各种资源进行质量监控。

（3）根据学校《广东软学院教师质量评价办法》及《广东东软学院教学质量管理体系实施办法》对课堂教学过程进行质量监控。

（4）根据学校《广东东软学院课程评估实施办法》及《广东东软学院课程考核工作管理办法》对课程和项目的各种形式考核进行质量监控。

（5）根据学校《广东东软学院实践学期及项目实训教学工作规范》及《广东东软学院实习实践教学质量检查办法》对学生参加实习和实践活动进行质量监控。

（6）根据学校《广东东软学院毕业设计（论文）工作管理办法》及《广东东软学院毕业设计（论文）工作质量评价办法》对学生毕业设计各个环节进行质量监控。

（7）专业教师的教学质量评价由 4 部分构成：教学资源（包括题库、案例库、项目库、教学平台、慕课等）建设、学评教、委员评教及同行评教。各部分所占比重每年根据侧重点不同可以有所调整。

3．教学质量评价机制

（1）实行教考分离原则，建立多元化考核体系，包括作业、在线测试、项目实践、期末考试等多种形式，全面评价学生学习效果。

（2）定期组织在校生进行教学满意度调查，收集并分析学生对教学内容、方法、资源等方面的反馈。

（3）建立毕业生跟踪反馈机制，通过校友会、社交媒体、职业发展调查等方式，收集毕业生对专业教学的长期反馈。

（4）引入第三方权威机构进行专业评估，结合行业报告和市场需求，评估人才培养质量。

（5）定期邀请企业合作伙伴、行业专家参与教学评估，从实际应用角度提供专业发展建议。

4．在校生、毕业生跟踪反馈及社会评价机制

（1）每年学生代表座谈，让学生就教师课堂教学进行反馈；

（2）学校招生就业办对毕业生就业数据形成了详细的分析报告，其中包含：毕业生的规模和结构、生源地、就业率、就业地区分布、就业行业分布、就业行业平均薪酬、就业指导服务满意度调查、毕业生就业满意度调查、学生就业意愿调查、家长就业意愿调查等，形成了调查报告，对专业的培养方案进行反馈和评价；

（3）对毕业 1 年以上的毕业生进行跟踪，以电话沟通、问卷调查、座谈、校友联谊等多种形式，根据在工作中遇到的问题，结合在校期间所学，对专业的教学体系进行反馈和评价。

5．人才培养质量持续提升机制

根据教育政策变化、工程教育认证标准更新、行业发展趋势，定期修订和完善网络空间安全专业的人才培养方案。建立课程与教学资源的定期更新机制，确保教学内容的前沿性和实用性。

实施“持续改进计划”，基于教学质量评价、学生反馈、校友及行业专家建议，不断优化教学计划和实践环节，提升人才培养质量。

十二、版本管理

版本号：Ver2025

制定小组成员：罗先录、孙伟、高艳芳、曾碧卿（华南师范大学）、钟昌乐（佛山大学）、植挺生（广东广宇科技发展有限公司）、吴栋（佛山市测绘地理信息研究院）、吴万钊（广东科信安信息技术有限公司）

系主任签字：罗先录

院长签字：罗先录

6. 教师及课程基本情况表

6.1专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
计算机导论	32	2	孙伟	大一第一学期
程序设计基础	80	6	周富肯	大一第一学期
程序设计基础课程设计	16	6	周富肯	大一第一学期
数据结构与算法	80	6	伍嘉华	大一第二学期
数据结构与算法课程设计	16	6	伍嘉华	大一第二学期
离散数学	64	4	刘卓敏	大一第一学期
操作系统原理	64	4	林瑾	大二第二学期
计算机网络	64	4	孙伟	大二第二学期
计算机组成原理	48	3	林瑾	大一第二学期
数据库系统原理	48	3	高艳芳	大二第一学期
网络空间安全概论	48	3	蒋镕泽	大二第一学期
计算机系统基础	64	4	罗先录	大二第二学期
人工智能基础	48	3	郭娟	大三第一学期
面向对象程序设计	48	3	卢丹娜	大二第一学期
专业导引与职涯规划（网络空间安全）	16	1	罗先录	大一第一学期
人工智能安全	64	4	郭娟	大三第二学期
密码学与网络安全	48	3	李智凯	大二第二学期
网络攻击与防范	48	3	李智凯	大三第一学期
软件系统安全	48	3	李晶	大二第二学期
Web安全技术	48	3	高艳芳	大二第二学期
网络协议编程	48	3	陈桂宏	大三第二学期
无线网络安全	32	2	蒋镕泽	大三第一学期
移动应用安全	32	2	卢丹娜	大三第一学期
电子取证技术	32	2	韩飞	大三第一学期
数据域内容安全	48	3	唐明	大三第二学期
逆向工程	32	2	李晶	大三第一学期

6.2本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历毕业学校	最后学历毕业专业	最后学历毕业学位	研究领域	专职/兼职
罗先录	男	1973-08	计算机系统基础、专业导引与职涯规划（网络空间安全）	教授	研究生	东北大学	计算机应用	硕士	系统安全、大数据分析，网络安全	专职
孙伟	男	1978-08	计算机导论、计算机网络	教授	研究生	东北大学	计算机应用技术	博士	数据库安全、网络攻防技术	专职
高艳芳	女	1983-02	数据库系统原理、Web安全技术	副教授	研究生	东北大学	计算机软件与理论	博士	软件安全、数据库安全	专职
周富肯	男	1981-07	程序设计基础、程序设计基础课程设计	教授	研究生	武汉大学	软件工程	硕士	软件安全、软件技术	专职
李晶	女	1987-01	软件系统安全、逆向工程	教授	研究生	华东师范大学	软件工程领域工程	硕士	Web安全、逆向分析与防护	专职
林瑾	女	1987-10	计算机组成原理、操作系统原理	教授	研究生	重庆大学	软件工程	博士	操作系统安全、嵌入式系统安全	专职
郭娟	女	1997-05	人工智能基础、人工智能安全	讲师	研究生	澳门理工大学	人工智能药物发现	博士	人工智能安全、可信计算、智能系统防御	专职
蒋镕泽	女	1983-04	无线网络安全、网络空间安	讲师	研究生	马来西亚理工学院	哲学PhD(AI方向)	博士	信息安全、AI安全	专职

			全概论							
韩飞	男	1969-07	电子取证技术	其他副高级	研究生	中国科学院计算技术研究所	计算机软件与理论	博士	通信安全、电子数据取证	专职
刘卓敏	女	1980-10	离散数学	未评级	研究生	匹兹堡大学	数学	博士	数据库安全、并行计算	专职
李智凯	男	1997-10	密码学与网络安全、网络攻击与防范	助教	研究生	湖北大学	网络空间安全	硕士	密码协议设计、安全策略分析	专职
伍嘉华	女	1981-01	数据结构与算法、数据结构与算法课程设计	教授	研究生	澳门科技大学	电子资讯科技	博士	算法安全、通信优化	专职
卢丹娜	女	1997-10	移动应用安全、面向对象程序设计	未评级	研究生	广州大学	网络空间安全	硕士	移动安全、软件工程安全	专职
唐明	男	1983-05	数据域内容安全	副教授	研究生	湖南大学	计算机应用	博士	信息隐藏与检测、通信系统安全	兼职
陈桂宏	女	1983-01	网络协议编程	副教授	研究生	中山大学	通信与信息系统	博士	无线网络安全、恶意代码分析	兼职

6.3教师及开课情况汇总表

专任教师总数	13		
具有教授（含其他正高级）职称教师数	6	比例	40.00%
具有副教授及以上（含其他副高级）职称教师数	10	比例	66.67%
具有硕士及以上学位教师数	15	比例	100.00%
具有博士学位教师数	10	比例	66.67%
35岁及以下青年教师数	3	比例	20.00%

36-55岁教师数	11	比例	73.33%
兼职/专职教师比例	2:13		
专业核心课程门数	26		
专业核心课程任课教师数	13		

7.专业主要带头人简介

<table>
<tr><td>姓名</td><td>罗先录</td><td>性别</td><td>男</td><td>专业技术职务</td><td>教授</td><td>行政职务</td><td>院长</td></tr>
<tr><td>拟承担课程</td><td colspan="3">计算机系统基础、专业导引与职涯规划（网络空间安全）</td><td>现在所在单位</td><td colspan="3">广东东软学院</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">2002年硕士研究生毕业于东北大学计算机应用技术专业</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">计算机系统安全、人工智能</td></tr>
<tr><td colspan="2">从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="6">1.广东省高校教学团队，广东东软学院系统能力教学团队负责人，结项；
2.教育部高校计算机类专业教指委第四批系统能力培养试点院校负责人，结项；
3. 教育部高等教育司：基于思科产学合作的计算机类主干课程综合改革,基于华为GaussDB数据库的实践实训课程建设，百度在线网络技术（北京）有限公司人工智能实验室建设负责人，均结项；
4，广东省一流本科专业软件工程,负责人，2021.02；
5. 2017-2022 主持广东省重点培育学科软件工程建设，180万，已结项；
6.第十届广东省高等教育教学成果一等奖，2022.05；
7.广东省一流本科课程，数据结构与算法，证书号202012192,2020.12；
8.广东省一流本科课程，计算机系统基础，证书号202210738,2022.10；
9.国家一流本科课程，程序设计基础，证书号2023241445,2023.5；
10.广东省本科高校人工智能教学指导委员会委员，2025.6
11.广东省计算机信息网络安全协会红帽人才专业委员会副主任委员、常务理事，广东省计算机学会网络空间安全专委会委员;
12. 南粤优秀教师</td></tr>
<tr><td colspan="2">从事科学研究及获奖情况</td><td colspan="6">1. 2023.1，广东省软件与信息服务工程技术研究中心，50万；；
2. 2022-今，教育部科技发展中心，中国高校产学研创新基金项目，无人机群协同应急测绘系统，20万；
3. 2023.1，佛山市科技局，佛山市无人机系统工程技术研究中心，10万；
4.广东省普通高校特色创新类项目”机器学习在安全攻防场景的应用与分析”，6万；网络安全技术与网络攻防实训平台建设，6万；
5，一种智能防疫用测温机器人，实用新型专利，ZL2021 2 2933197.2；
6，基于Topsis算法的疫情监控系统，计算机软件著作权，2021SR2151978；
7. 基于计算机系统能力培养的程序语言选用分析[J]，软件工程</td></tr>
</table>

	,2020,23(11) 8. The Myth of Disassembly and Reverse Engineering Based on a Digital Signature Scheme, Design Engineering, Issue 2,2021 9. 鹏城实验室新安盟靶场技术专委会委员；主持佛山市卫健行业网络安全竞赛； 10.佛山市计算机学会副会长,佛山市人工智能学会副会长。		
近三年获得教学研究经费（万元）	200.0	近三年获得科学研究经费（万元）	80.0
近三年给本科生授课课程及学时数	1.《数据结构与算法》，256课时； 2.《程序设计基础》，192课时； 3.《计算机系统基础》，192课时。	近三年指导本科毕业设计（人次）	20

姓名	孙伟	性别	男	专业技术职务	教授	行政职务	校长
拟承担课程	计算机导论、计算机网络			现在所在单位	广东东软学院		
最后学历毕业时间、学校、专业		2010年博士毕业于东北大学计算机应用技术					
主要研究方向		网络安全、无线网络协议性能分析					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		1.辽宁省泛在网络安全与计算技术创新团队执行负责人 2.2022年作为广东省重点培育学科软件工程带头人，负责学科建设和相关验收工作； 3.2020年作为“面向应用型人才培养的智慧化混合式教学模式研究与实践”主要完成人获辽宁省教育厅教学成果一等奖； 4.2020年作为“基于TOPCARES-OBE的工程型软件人才培养的综合改革与实践”第一完成人获辽宁省教育厅教学成果二等奖； 5.2019年获辽宁省高等学校创新人才； 6.2018年作为“一体化IT类应用型创新创业人才培养体系的改革与实践”主要完成人获辽宁省教育厅教学成果一等奖； 7.深化基于 ‘校-小企业联盟’的计算机专业实践教学，培养创新创业应用型人才” 第一完成人获辽宁省教育厅教学成果二等奖； 8.2014年，获国家留学基金委“CSC－IBM中国奖研金” 一等奖； 9.2013年，获得“ 基于TOPCARES-CDIO的IT类人才培养体系的探索与实践”辽宁省教学成果奖一等奖(主要完成人)；					

<table>
<tr><td>从事科学研究及获奖情况</td><td colspan="7">1.广东省软件与信息服务工程技术研究中心负责人，2022；
2.广东省重点培育学科软件工程，学科带头人，2022
3.辽宁省高等学校创新人才，2019；
4.辽宁省大数据应用研究重点实验室，负责人，2019；
5.国家自然科学基金项目“无线传感器网络内部恶意节点识别关键技术研究”；
6.辽宁省博士启动基金“无线传感器网络中跨应用资源调度技术研究”(20170520398)
7.国家自然科学基金项目“3GPP框架下UMTS核心网安全问题的研究”；
8.2017 年成果转化《大连港物业系统开发》,大连宏誉大厦有限公司
9.2016 年成果转化《慢性病患者基础医疗数据采集及移动智能监控综合系统的研发》,大连东软思维科技发展有限公司
10.基于自适应直方图修改的网格可逆信息隐藏. 东北大学学报（自然科学版）2020.
11.Semi-Supervised Self-Training Feature Weighted Clustering Decision Tree and Random Forest. IEEE ACCESS 2020；
12. A multimodal emotion recognition model integrating speech, video and MoCAP，Multimedia Tools and Applications，2022
13. 融合说话者特征的个性化自然语音情感识别，计算机应用与软件，2022；</td></tr>
<tr><td>近三年获得教学研究经费（万元）</td><td colspan="3">8.0</td><td>近三年获得科学研究经费（万元）</td><td colspan="3">210.0</td></tr>
<tr><td>近三年给本科生授课课程及学时数</td><td colspan="3">计算机网络，128课时</td><td>近三年指导本科毕业设计（人次）</td><td colspan="3">21</td></tr>
</table>

<table>
<tr><td>姓名</td><td>高艳芳</td><td>性别</td><td>女</td><td>专业技术职务</td><td>副教授</td><td>行政职务</td><td>佛山市智能软件工程技术研究中心主任</td></tr>
<tr><td>拟承担课程</td><td colspan="3">数据库系统原理、Web安全技术</td><td>现在所在单位</td><td colspan="3">广东东软学院</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">2020年10月毕业于东北大学计算机软件与理论专业，获工学博士学位</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">数据分析、人工智能、区块链、软件工程等领域</td></tr>
</table>

从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	[1] Multiple Teaching Objectives-oriented Automatic Test Paper Generation System, 2024 3rd International Conference on Artificial Intelligence and Education (ICAIE 2024) , November 22-24, 2024, Xiamen, China (ISBN: 979-8-4007-1269-2), ACM; [2] 全国高等学校计算机教育研究会，基于OBE理念的计算机类专业《程序设计基础》课程思政体系研究与实践(编号:CERACU2022R25)，2022年7月； [3] 参编教材:《互联网技术》，副主编，2021年9月出版，东北大学出版社，34.8万字，ISBN 978-7-5517-2694-8; [4] 2024年、2025年连续两年获校级优秀指导教师荣誉； [5] 2012年获工程师职称、2013年通过PMP项目管理资质、2024年通过中科院心理研究所心理咨询师考试。
从事科学研究及获奖情况	[1] Research on Short Text Speech Understanding Methods for Factory Applications, 2024 4th International Conference on Electronic Information Engineering and Computer Science (EIECS), Yanji, China, 2024, (ISBN: 979-8-3315-3140-9), IEEE, (EI检索: 20250517786810) [2] 基于区块链的无线体域网数据云存储完整性研究,2020年,东北大学学报(10053026), (EI检索：20201608430952),东北大学(中文核心) [3] Research of Query Verification Algorithm on Body Sensing Data in Cloud Computing Environment，2019年，Web Information Systems and Applications (978-3-030-30951-0)，Springer（EI检索：20194807760641） [4] Research on Computing Verification Algorithm on Body Sensing Data in Cloud Computing Environment，2019年，Jornal of Physics Conference Series(1742-6588)，IOP Publishing（EI检索：20194907794716） [5] Research on Security for Wireless Body Area Network Data in Cloud Storage Based on Blockchain,2019年,Jornal of Physics Conference Series(1742-6588),IOP Publishing（EI检索:20194907794758） [6]辽宁省工业和信息化厅项目，基于AI模型和心音重构技术的心血管检测仪，2025年3月 [7] 国家自然科学基金项目,智慧城市大规模位置数据发布中的轨迹隐私保护技术研究,(批准号:61602106),2017年5月-2020年4月 [8] 中国高校产学研创新基金项目，“边缘计算”模式下的智能体（机器人

	）协同运动控制(编号：2021LDA02002),2023年 [9] 广东省高等教育学会课题，人工智能发展时代下的学生课堂注意力研究(编号：24GQN30),2024年5月 [10] 佛山市社会科学界联合会，基于大数据的青年思想动态研究(编号:2024-QNFZ18)，2024年4月		
近三年获得教学研究经费（万元）	5.0	近三年获得科学研究经费（万元）	45.0
近三年给本科生授课课程及学时数	1、操作系统，64学时； 2、数据库系统原理，192学时； 3、人工智能基础，96学时；	近三年指导本科毕业设计（人次）	30

8.教学条件情况表

可用于该专业的教学实验设备总价值（万元）	760.68	可用于该专业的教学实验设备数量（千元以上）	102（台/件）
开办经费及来源	600万 各类学科建设经费及学校自筹		
生均年教学日常运行支出（元）	4255.04		
实践教学基地（个）	16		
教学条件建设规划及保障措施	严格遵照教育部《普通高等学校基本办学条件指标(试行)》要求,确保生均教学行政用房、生均教学科研仪器设备值、生均年教学日常支出、生均图书、实践教学基地数量等指标符合基本办学条件和核定年度招生规模。多渠道筹措建设资金，不断改善、更新教学条件，提高教学质量和高等学校信息化程度。 加强实验室建设，要使实验室的基本设备条件以及教学内容等方面得到进步的提高，能够更多开出一批反映科技最新发展的新型实验和众多反应网络空间安全技术实战型实验;使一大批综合性、设计性实验成为实验的主要内容和主要实验教学方式。完善核心课程课堂演示实验教学。通过已建成的网络空间安全产业学院、大数据产业学院吸纳更多的优质企业，对接地方企业的人才需求;继续完善实践体系，加大实践基地建设的力度，使每个实践环节真正落到实处，起到应有的效果。		

9. 申请增设专业的理由和基础

申请增设专业的理由和基础

（专业名称：网络空间安全 专业代码：080911TK）

一、增设网络空间安全专业的主要理由

没有网络安全，就没有国家安全。网络空间作为大国战略博弈的主战场，其安全已成为国家安全的核心支柱。习近平总书记近年来持续强调网络安全人才培养的战略意义，并明确指出，建设网络强国需要高素质的网络安全和信息化人才队伍。

当前，随着人工智能、量子计算等新技术的发展，网络安全威胁呈现智能化、复杂化特征。根据工业和信息化部《网络安全产业高质量发展三年行动计划（2023-2025）》（工信部网安〔2023〕76 号），我国网络安全人才缺口已突破 300 万，其中粤港澳大湾区人才需求占比达 20%以上。根据广东省政府《'数字湾区'建设三年行动方案》，到 2025 年将新增 5 万个网络安全专业岗位，重点覆盖人工智能安全、跨境数据保护等国家急需领域（粤府〔2023〕36 号）。人力资源和社会保障部 2024 年发布的《数据安全工程技术人员国家职业标准》，首次确立了网络安全人才的职业认证体系。国内政企机构对网络安全的重视程度日益提高，对网络安全人才的需求日益增长。网络空间的竞争，归根结底是人才竞争，网络空间安全不仅需要具有研究能力和创新精神的科研工作者，更需要各层次网络空间安全人才的支撑。

专业设置和专业建设是体现高等学校市场应变能力的重要环节，是高校发展的核心和根本。根据国家及广东省对网络空间安全人才的需求，以及广东东软学院的办学特色与优势，结合学校的专业发展规划，在充分调研基础上，特申请设置网络空间安全本科专业。

（一）培养网络空间安全人才是国家安全与国民经济发展需要

在数字化浪潮席卷全球的今天，网络空间安全已成为关乎国家长治久安和经济社会高质量发展的战略性议题。随着新一代信息技术的快速发展和广泛应用，网络安全威胁正呈现出跨国界、跨领域的新特征，对国家安全和经济发展构成严峻挑战。在此背景下，培养高素质网络空间安全人才，不仅是筑牢国家安全防线的必然要求，更是推动数字经济发展的关键支撑。

从国家安全的战略高度来看，网络空间安全人才培养直接关系到国家主权和核心利益的维护。近年来，国际网络空间博弈日益激烈，网络安全威胁持续升级。面对日益复杂的网络安全形势，中央网信办等 13 部门联合发布的《网络安全审查办法（2023 年修订）》（国家互联网信息办公室令第 14 号）明确要求关键信息基础设施运营者必须建立专业网络安全团队，配备符合要求的专业技术人才。这一制度性安排凸显了网络安全人才培养在国家治理体系中的战略地位。同时，人力资源和社会保障部 2024 年发布的《数据安全工程技术人员国家职业标准》，首次将网络安全人才纳入国家职业资格认证体系，为专业化人才培养提供了制度保障。这些政策法规的密集出台，充分体现了国家对网络安全人才培养的高度重视，也为高校增设网络空间安全专业指明了方向。

网络安全人才培养是推动产业转型升级的重要支撑。随着数字经济成为经济增长的新引擎，网络安全已成为保障产业数字化转型的基础条件。中国信息通信研究院《中国网络安全产业白皮书（2024）》显示，2023 年我国网络安全产业规模达到 2235 亿元，同比增长 28.6%，但专业人才供需矛盾日益突出，人才缺口高达 327 万人。特别是在工业互联网、智能网联汽车

等新兴领域，人才供需比达到 1:8 的严重失衡状态。这种结构性短缺直接制约着企业的数字化转型进程和创新发展能力。以粤港澳大湾区为例，广东省政务服务数据管理局统计数据显示，2023 年区域内网络安全岗位需求同比增长 42%,其中数据安全分析师、云安全架构师等新兴职位占比超过 35%。为应对这一挑战,广东省"数字湾区"建设三年行动方案(粤府〔2023〕36 号）明确提出未来三年将新增 5 万名持证网络安全专业人才，重点服务智能制造、跨境金融等特色产业。这些数据充分表明，系统化培养既懂网络安全技术又了解产业需求的复合型人才，已成为推动区域经济高质量发展的迫切需求。

网络安全人才培养既是维护国家安全的战略需要，也是推动数字经济高质量发展的核心支撑。建设网络空间安全本科专业，系统培养掌握核心技术、具备实战能力的高层次人才，既是应对当前国家安全挑战的战略选择，更是服务数字中国建设的长远布局。通过构建完善的网络安全人才培养体系，能够为国家网络安全防线建设提供坚实人才保障，同时为数字经济发展注入持续动力。因此，建设网络空间安全本科专业，培养网络空间安全高层次人才就显得尤为重要。

（二）培养网络空间安全人才是科技自立自强的战略需要

在全球科技竞争日益激烈的背景下，网络空间安全人才的培养已成为实现科技自立自强的关键战略支点。当前，我国正面临着从"跟跑"到"并跑"乃至"领跑"的科技发展转型期，而网络安全作为基础性、战略性支撑领域，其人才培养直接关系到核心技术突破和产业链安全。根据科技部《"十四五"国家科技创新规划》的部署，网络安全已被列为需要重点突破的七大前沿

领域之一，与人工智能、量子信息等并列成为国家战略科技力量建设的重要组成部分。这一战略定位凸显了网络安全人才培养在国家创新体系中的特殊重要性。

网络安全人才培养是破解"卡脖子"难题的重要突破口。中国工程院《2023 年网络空间安全发展报告》显示，在芯片设计、操作系统等关键领域，约 68%的技术封锁都涉及安全专利壁垒。以华为鸿蒙操作系统研发为例，其成功突破的关键在于组建了超过 2000 人的专业安全团队，这些人才不仅解决了系统级的安全问题，更在微内核架构、形式化验证等核心技术上实现了从 0 到 1 的突破。同样，在国产 CPU 研发过程中，网络安全专家主导设计的安全防护模块，使得"龙芯"等自主芯片产品能够有效抵御各类硬件级攻击，为国产芯片的规模化应用扫清了安全障碍。因此，没有自主培养的网络安全人才队伍，就难以实现真正意义上的技术自主可控。

在构建完整创新生态方面，网络安全人才培养发挥着不可替代的纽带作用。教育部"特色化示范性软件学院"的建设经验表明，通过校企联合培养的网络安全人才，正在成为连接基础研究、技术开发和产业应用的关键力量。以阿里云主导的"龙蜥"操作系统开源社区为例，其核心安全团队中 75%的成员毕业于国内高校网络安全相关专业，这些人才不仅具备扎实的理论功底，更拥有丰富的实战经验，能够将学术界的最新研究成果快速转化为产业可用的安全解决方案。

因此，培养网络空间安全人才是实现科技自立自强的战略需要。网络安全领域的科技攻关具有鲜明的复合型特征，既需要培养能够开展基础理论创新的战略型人才，也需要造就具备解决"卡脖子"技术难题能力的实战型

人才。实践证明，增设网络空间安全专业，建立完善的人才培养体系，是突破技术封锁、构建安全可控技术体系的重要保障，更是实现高水平科技自立自强的必由之路。

（三）培养网络空间安全人才急需设置网络空间安全专业

伴随着信息化的快速发展，网络安全问题更加突出，对网络安全人才建设不断提出新的要求。网络空间的竞争，归根结底是人才竞争。因此，积极构建网络空间安全学科体系，使我国网络信息安全人才成体系化、规模化、系统化培养，才能更好地满足国家安全对网络信息安全人才的需要。

从人才需求来看，网络安全领域存在显著的技能缺口，尤其在云计算安全、人工智能、机器学习等新兴技术领域，高层次、复合型人才相对匮乏。据《2024 年网络安全产业人才发展报告》显示，全球网络安全人才缺口持续扩大，技能缺口明显，国内网络安全人才市场也受到经济形势的影响，人才结构性矛盾突出。报告指出，本科学历人员一直是网络安全岗位的主力军，占比约 58.2%，硕士研究生及以上学历人才占比 11.6%，专科学历人才占比 30.2%。随着数字化转型的加速，未来 3-5 年网络安全人才的需求增长率将保持在 20%以上，新兴领域的缺口将进一步扩大。

网络空间安全学科的建设，是培养高层次创新型人才的关键。2015 年 6 月，国务院学位委员会、教育部批准增设“网络空间安全”一级学科，标志着我国网络安全人才培养进入体系化发展阶段。2017 年，中央网信办、教育部联合启动“一流网络安全学院建设示范项目”，推动 21 所高校加强网络安全学科建设。这些举措有效提升了我国网络安全人才培养质量，但仍存在覆盖面不足、培养规模有限等问题。因此，扩大网络空间安全专业的设

置范围，优化课程体系，加强校企合作，是当前网络安全人才培养的必然选择。与此同时，现有网络安全人才培养模式存在学科分散、课程体系不完善、实践能力不足等问题。许多高校将网络安全课程分散在计算机科学与技术、信息安全等专业中，导致学生知识结构碎片化，难以适应实战需求。美国国家标准与技术研究院（NIST）在《国家网络安全教育倡议（NICE）》中明确提出，网络安全应作为独立学科，并强调实践能力培养。因此，加快网络空间安全专业建设，以系统化、专业化方式培养高素质网络安全人才就显得尤为重要。

当前，国家对网络空间安全人才的需求是全方位的，既包括网络空间安全战略人才、网络安全与信息科技领军人才、网络安全和信息技术工程人才、网络安全分析人才，也包括网络安全管理、运行维护人员和技能型操作使用人员等，因而对于网络空间安全人才的培养体系也必定是全方位、多层次的，只有在网络空间安全一级学科规范下，按照博士、硕士和学士成体系培养，才能全方位地满足国家对于网络空间安全各类人才的需求。

因此，设置网络空间安全本科专业，对实现网络空间安全人才培养是重要而且必要的。既是国家安全战略的迫切需求，也满足国家及省市大力发展工科的需要，势在必行。

（四）广东东软学院设置网络空间安全专业的优势与特色

广东东软学院是经国家教育部批准设立，由大连东软控股有限公司、亿达集团有限公司共同投资举办的一所民办普通高等院校，地处粤港澳大湾区的核心区域。主要培养面向粤港澳大湾区的高素质应用型人才。

1.学科及专业特色优势

广东东软学院在信息技术领域积累了多年的办学经验，拥有 2 个与网络空间安全相关的广东省重点学科——软件工程、管理科学与工程学科。并在网络安全、大数据安全、计算机软件与理论、以及教育、医疗、电子政务等应用软件领域开展特色鲜明的研究。学校还设有网络工程、软件工程等相关专业，拥有省级实验教学示范中心和省级大学生校外实践基地等教学平台，为专业建设提供了坚实的基础。其中，网络工程专业是广东省特色专业，是广东省财政厅、教育厅 2018 年省级教育发展专项资金（民办教育发展方向）建设专业，主要培养 IT 领域中计算机和信息安全交叉学科应用型人才。该专业团队是广东省公安厅授权的“红帽先锋队”，多次承担省公安厅分配的护网任务，并受到广东省及各市公安局的表扬信若干。



感 谢 信

广东东软学院：

由广东省委网信办、广东省公安厅、广东省政务服务和数据管理局、广州市委网信办、广州市政务服务和数据管理局指导，广州市公安局、黄埔区公安分局、黄埔区委网信办、黄埔区政务服务和数据管理局联合主办的“埔剑杯”之 2024 · 赋能新质生产力网络安全实战攻防演练于 2024 年 6 月 25 日至 2024 年 7 月 4 日顺利举办。

在演练举办期间，贵单位给予大力支持，积极选派骨干技术人员参与其中，充分施展技术特长，发挥技术支撑作用，圆满完成了本次实战演练任务。

在此特向贵单位及相关技术人员表示衷心感谢，期望贵单位继续为网络安全建设工作提供更多优质服务，推动全社会网络安全保障能力持续提升。

广东省公安厅网络警察总队
2024 年 9 月

广州市公安局网络警察支队
2024 年 9 月

广州市公安局黄埔区分局
2024 年 9 月

惠州市政务服务和数据管理局

感谢信

广东东软学院：

为深入贯彻网络强国战略，全面检验我市数字政府网络安全防护和应急处置能力，我市于 2024 年 6 月 17 日至 25 日举办了“惠盾—2024”惠州市数字政府网络安全攻防演练。本次演练有效检验了我市数字政府网络安全整体防护能力，为我市主动防御、快速处置大面积政务网络攻击事件积累了经验、形成了能力。

贵单位作为本次演练的技术支撑单位，表现出专业性强、技能全面、工作积极负责的特点，充分体现了贵单位的责任担当。同时，贵单位的庞永棋、周国营、罗东同志利用自身专业知识作为红方队员参演，打出了网络攻击队的气势与专业，为活动的高标准、高质量举办提供了鼎力支持。

在此，我局谨向贵单位致以最诚挚的谢意，并对以上同志提出表扬，希望他们在今后的工作中再接再厉。请贵单位继续支持我市数字政府网络安全工作，共同促进我市数字政府网络安全水平稳步提升！

惠州市政务服务和数据管理局
2024 年 7 月 15 日

2.“产教融合”办学特色

在网络空间安全专业的建设中，学校充分发挥“产教融合”的办学特色，通过与产业界深度合作，构建了多元化的协同育人机制，为学生提供了丰富的实践机会和前沿的行业知识。学校依托东软集团的深厚产业背景，借助其在信息技术领域的丰富资源和实践经验，为学生打造了从理论学习到实践应用的完整培养链条。

广东东软学院联合奇安信科技集团建成了网络空间安全产业学院、联合东软集团建成了大数据产业学院。依托 75 个教育部产学合作项目，与企业共同申报课题研究、技术服务、产品研发、专利申报等 97 项；建成省教育厅网络安全技术与网络攻防实训平台；成立省公安厅授权的“红帽先锋队”，参加公安厅护网、广交会、粤盾、极盾等 83 场次，师生获得表彰 120 余人次，成为维护国家安全的可靠力量；承办广东省高校“东软杯”网络攻防大赛 7 次；为中国移动广东分公司提供网络安全技术培训 11 场次；承办 2 次卫生健康行业网络安全技能与培训。

南海区公安局与佛山市南海区大数据协会协调多方资源探索组建了全省首支网络和数据安全服务队，旨在通过资源整合、协同响应和技术赋能，提升区域网络安全防护能力，护航数字经济发展。广东东软学院作为成员之一，积极参与了网络安全服务工作。2024 年，广东东软学院计算机学院被评为南海区网络和数据安全服务工作“突出贡献企业”和“优秀成员单位”。学院积极开展网络安全工作，例如在校内举办主题宣讲，面向中小学开展知识普及，与政府部门合作举办专题讲座并参与网络安全服务

队工作。学院还组织学生参加网络安全竞赛，在南海区攻防演练中获得多项奖项，有效提升了网络安全人才培养质量。



3.研究方向及主要贡献

（1）科学研究方面：承担了广东省“智能制造领域新型边缘云协同系统关键技术研究及应用”、“复杂场景下MIMO雷达近场目标参数估计方法研究”等省部级项目47项。并且在网络安全、大数据安全、计算机软件与理论、以及教育、医疗、电子政务等领域的应用软件等方面的研究取得了较好的成果。近三年，网络安全师资团队，在IET Computer Vision、Future Generation Computer Systems等期刊和IEEE与ACM等会议上发表了SCI/EI论文29篇篇；申请发明专利31件、授权实用新型专利9件。

（2）团队建设方面：广东东软学院拥有一支高水平的师资队伍，教授和讲师们不仅具备扎实的学术背景，还在网络安全领域有着丰富的实践经验。许多教师参与过国家级科研项目，并与国内外知名网络安全公司保持紧密合作，具有前沿的学术视野和行业洞察力。建成了一支以网络安全师资为核心的校级优秀教师团队，团队中包括专任教师13人，外聘教师2人，其中南粤教师1人，省民办优秀教师2人，省公安厅“优秀红帽指导

老师”1 人，校级优秀教师 5 人。近三年，在“第一届全国教学数字化大赛国赛”、“第五届混合式教学设计创新大赛”、“第六届青年教师教学大赛”等省部级以上教师教学竞赛中获得 15 个奖项。

（3）学科竞赛方面：学校鼓励学生积极参加各种竞赛，近三年，获得的 127 项计算机类竞赛奖项，其中国家级 12 项、省级 115 项，主要包括蓝桥杯大赛（72 项）、全国高校计算机能力挑战赛（21 项）等赛事。国家级奖项包括数据挖掘与 AI 建模大赛、中国大学生计算机设计大赛、“盘古石杯’国际电子数据取证大赛等，由广东省网络空间安全协会、教育部等机构颁发；省级奖项包括华为中国大学生 ICT 大赛、“传智杯”全国大学生 IT 技能大赛、C4 网络技术挑战赛等。



（4）人才培养方面：每年培养毕业网络工程（网络安全方向）本科学生 200 余人，其中近 3 年有 22 人考研成功，考取了暨南大学、广州大学、广东工业大学等大学的硕士研究生，平均就业率在 90%以上。本科人才的培养依托网络工程、软件工程等相关专业及方向，已经形成了较为完

整的人才培养计划与课程体系，并撰写出版了《密码学与网络安全》、《网络工程综合实践教程》等多部相关教材。获教育部“系统能力培养”试点院校；教育部-思科产学育人项目获全国优秀项目，并通过中国高等教育学会在全国57所高校推广，得到广泛认可。人才培养模式创新成果《产学、项目、导师三制式创新人才培养体系探索与实践》获省级教学成果二等奖，《双平台、双核心、双情景，网络安全人才培养模式的创新与实践》获校级教学成果一等奖。

二、学校专业发展规划

广东东软学院以社会经济发展需求为导向，以学科发展为基础，优化学科专业结构，形成布局科学、结构合理、具有自身特色和优势的本科专业体系增设适应国家发展战略需要并有利于形成集群优势的新兴交叉专业，全面提高人才培养质量，为广东省更充分地培养珠三角网络安全应用型人才培养空白。在未来五年的发展规划中，广东东软学院网络空间安全专业将致力于实现稳步增长的在校生规模和层次分明的建设目标，以满足社会对网络空间安全人才的迫切需求，并不断提升专业的教学与科研水平。申请增设“网络空间安全”本科专业，是落实广东省“新工科”建设与产教融合政策的重要举措，是广东东软学院响应《网络安全法》和《国家网络空间安全战略》的具体行动。

计算机学院是广东东软学院规模最大的二级学院，设有软件工程、网络工程等六个本科专业。学院建有26个专业实验室，包括网络空间安全与攻防实验室，并与企业共建了东软百度人工智能学院、奇安信网络空间安全产业学院等实践平台。目前，拥有一支年龄结构合理、学科分布均衡的从事网

络空间安全教学与科研工作的师资队伍，专职教师 13 人，其中教授 5 人，副教授 3 人，讲师 2 人，高级职称教师人数占 61.5%，具有博士学位的 8 人，符合《普通高等学校本科专业类教学质量国家标准》要求。

广东东软学院网络空间安全专业建设的基本思想是以国家网络安全与信息化战略为指导，以服务于国家战略产业与区域经济发展为前提，以软件工程网络工程等相关学科与专业为依托，按照学校的学科与专业发展规划，统筹与整合相关的教学资源，积极探索课程体系与教学方法，集中力量建设具有产业特色的网络空间安全多元化、多层次人才培养体系为了适应当前科技变革和产业变革加速进行、国际竞争日趋激烈的现状推动网络空间安全专业新工科建设，在网络空间安全专业的建设过程中深入推进产学合作、产教融合、科教协同，通过与奇安信集团、深信服、东软集团等知名企业的合作，共同建设网络空间安全专业。具体措施有共建产业学院、校企联合制定培养目标和培养方案、共同建设课程与开发教程、共建实验室和实训实习基地、合作培养培训师资、合作开展研究等，引入行业企业参与到教育教学各个环节中，促进人才培养与产业需求紧密结合。

根据《普通高等学校本科专业类教学质量国家标准》对网络空间安全的知识体系的要求,预计建立的网络空间安全本科专业课程体系如图1所示。

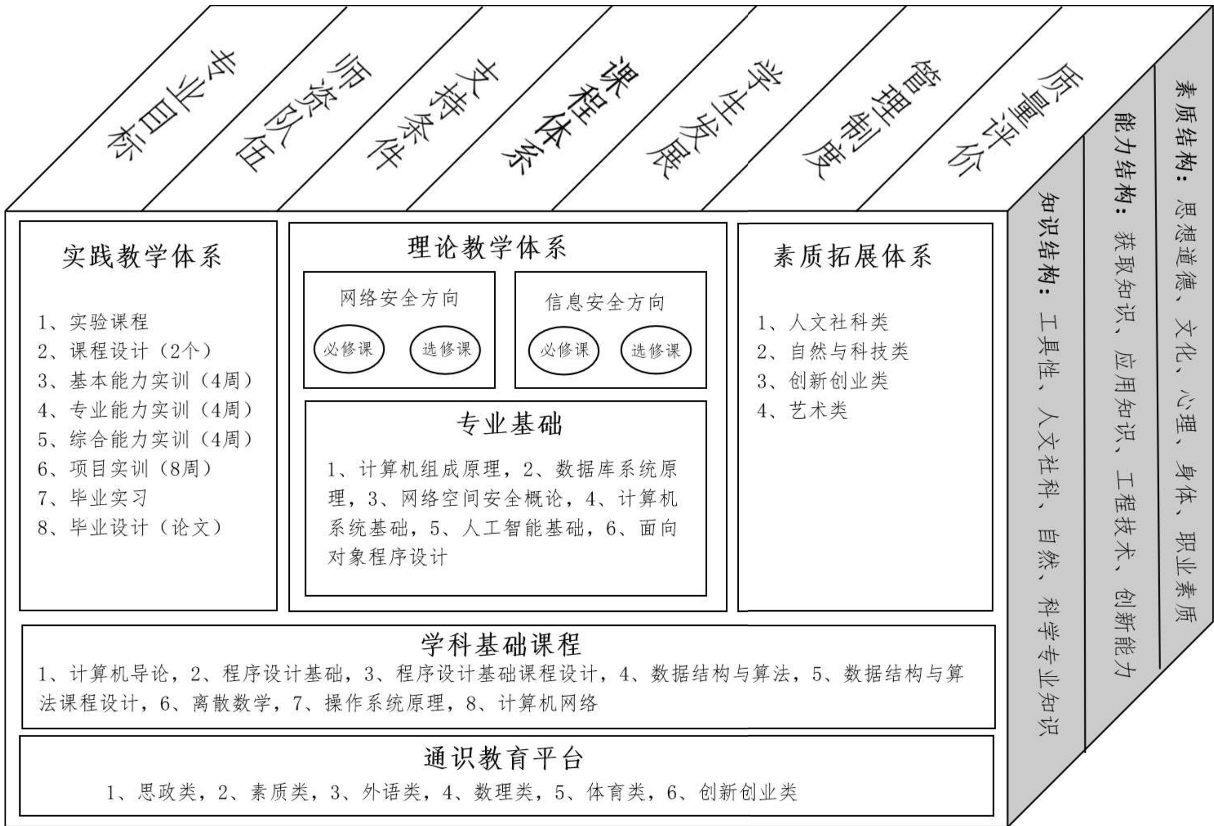


图1 网络空间安全本科专业课程体系

网络空间安全的知识体系涵盖了网络空间安全基础、密码学及应用、系统安全、网络安全、信息系统安全和信息内容安全等知识领域的内容，是以跨学科凝练的安全基本理论体系和方法论来指导多学科安全问题研究的完整体系，因此，网络空间安全专业的培养计划和课程体系建设应以安全基本理论体系和方法论为指引,在广东东软学院本科专业通识教育和学科教育教学要求的基础上，依据本专业的培养目标，设置相应的专业基础课、专业方向课、专业选修课，以及相关的实践性教学环节，

根据《普通高等学校本科专业类教学质量国家标准》对网络空间安全的知识体系的要求，预计建立的网络空间安全本科专业课程体系，课程体系涵

盖了网络空间安全所涉及的数学、数字电子、计算机科学与技术、信息论、控制论、博弈论、密码学理论和网络空间安全法律法规等需要学生掌握的基础理论知识，为此，设置了计算机导论、程序设计基础、程序设计基础课程设计、数据结构与算法、数据结构与算法课程设计、离散数学、操作系统原理和计算机网络等课程，网络空间安全专业知识涵盖了支撑网络空间安全技术及其应用所涉及的网络空间安全及相关的学科领域的专业知识，其中，相关领域知识群的课程有计算机组成原理、数据库系统原理、网络空间安全概论、计算机系统基础、人工智能基础和面向对象程序设计等；网络空间安全领域知识群的课程有网络安全和信息安全。

网络空间安全应用技术涵盖了解决网络空间安全工程领域复杂问题所涉及的相关安全 技术与方法，为此，设置了专业导引与职涯规划（网络空间安全）、人工智能安全、密码学与网络安全、网络攻击与防范、软件系统安全、Web 安全技术等。

在实践性教学环节方面，课程设计、网络空间安全综合实验、科研/竞赛训练等实践教学环节贯穿课程体系的始终,使得学生能够通过实践教学环节的不同类型实验,进一步理解与掌握网络空间安全的相关知识,提高其独立分析与解决问题的实践能力。毕业实习和毕业设计环节则通过相关课题的分析、研究、设计与实现过程,对学生解决网络空间安全工程领域复杂问题的综合能力进行培养和锻炼。

广东东软学院联合奇安信科技集团新建成了网络空间安全实验室、体验式网络安全展厅，扩建了网络工程实验室、网络攻防实验室,能够提供各种类型的网络空间安全实验,并支持各类相关新实验的开设，能够同时支持

300 人的实验实训。进一步提升佛山市网络信息应用安全工程技术研究中心和信息安全研究所等科研平台建设水平，争取申报获批广东省网络与信息安全工程实验室建设。推动本专业建设成为教学科研设备先进、具有省内先进水平的高层次人才培养和科研教学、技术培训基地。组织有专业潜力、动手能力较强的学生进入实验室开展特定项目的训练。

综上所述，网络空间安全一级学科点的设立体现了这一科学领域的重要性和国家对相关人才的迫切需求,符合网络空间安全专业要求的技术人才仍然十分短缺，广东东软学院具有开设网络空间安全专业的优势和基础，并已经形成了“网络安全”专业方向的鲜明专业特色和优势，广东东软学院完全有能力办好网络空间安全专业。通过几年的努力与建设，可以将本专业建设成为政治思想坚定、培养方案科学、课程体系合理、师资队伍稳健和教学实践资源丰富的特色专业，成为国家和社会重要的网络空间安全专业优秀人才培养基地，而且为中国的安全产业的发展输送具有思想过硬、理论基础坚实、实践技能丰富和创新思维能力优秀的网络空间安全专业人才。

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

总体判断拟开设专业是否可行		☑是 □否
理由： 按照教育部《普通高等学校本科专业设置管理规定》等文件的要求，对照《普通高等学校本科专业类教学质量国家标准》，广东东软学院专业设置评议专家组对“网络空间安全”专业设置事宜进行了评审，专家组一致认为： 该专业面向国家网络强国战略及粤港澳大湾区数字经济安全需求，可为区域金融、医疗、制造等重点行业输送急需的网络安全运维、攻防与数据安全人才，是学校主动服务《网络安全法》《“十四五”国家信息化规划》的关键举措；专业建设方向契合学校 IT 应用型办学定位，可依托现有专业共享课程和实验资源，并与东软集团在安全产品研发、医疗数据防护等方面的产业优势深度产教融合。 该专业符合学校的发展定位和学科专业发展规划；人才培养方案科学规范；现有专业可以很好的支撑该专业的建设；专业师资队伍职称、学历、年龄结构合理，专业负责人资历符合专业建设需求；教学用房、图书资料、攻防演练实验室、渗透测试平台等教学条件完备；学经费充足，管理制度健全，满足专业可持续发展的基本条件。 专家组一致同意申报“网络空间安全”专业。		
拟招生人数与人才需求预测是否匹配		☑是 □否
本专业开设的基本条件是否符合教学质量国家标准	教师队伍	☑是 □否
	实践条件	☑是 □否
	经费保障	☑是 □否
专家签字：		